

Privacybeleid



Revisie

Versie	Datum	Status	Geaccordeerd
0.1	01-03-2025	Definitief	29-04-2025

Auteurs: Tjalle ter Stege FG

Reviewdatum: 01-01-2028



Inhoudsopgave

.....	1
Inhoudsopgave	3
1. Aanleiding.....	4
2. Begripsbepalingen.....	4
3. Visie	4
4. Doel	5
5. Reikwijdte.....	5
6. Principes van de verwerking	6
7. Rollen en verantwoordelijkheden	10
8. Overlegstructuur	13



1. Aanleiding

De Westerkim werkt met (Persoons)gegevens van cliënten, medewerkers en (keten)partners. Deze gegevens verzamelt De Westerkim voor het goed kunnen uitvoeren van de zorgtaken. Om deze taken goed te volbrengen is het noodzakelijk dat De Westerkim persoonsgegevens verwerkt. Cliënten, medewerkers en andere betrokkenen moet erop kunnen vertrouwen dat De Westerkim zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaal wordende samenleving maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De Westerkim is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Geldigheidsduur

Dit beleid is vastgesteld op <datum> door de Raad van Bestuur. Het beleid wordt tenminste een keer per vier jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld in geval van grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's, o.i.d.) kan de Raad van Bestuur besluiten tot een tussentijdse herziening.

2. Begripsbepalingen

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

3. Visie

De komende jaren zet De Westerkim in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van De Westerkim en de basis voor het beschermen van rechten van betrokkenen zoals cliënten en medewerkers. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van medewerkers essentieel voor privacy binnen De Westerkim.



4. Doel

Met dit privacybeleid geeft De Westerkim een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan De Westerkim persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen De Westerkim, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken en rechten van betrokkenen.

Naast dit door de Raad van Bestuur vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het privacybeleid kan daarom niet los worden gezien van het informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen De Westerkim is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De Westerkim verlangt van al haar medewerkers en alle personen die werkzaam zijn voor De Westerkim dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte

De Westerkim verzamelt en gebruikt persoonsgegevens van cliënten, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens De Westerkim, waaronder:

- De verwerking van persoonsgegevens binnen de bedrijfsprocessen van De Westerkim;
- De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van De Westerkim aan een rechtspersoon die voor De Westerkim bepaalde diensten verricht;
- De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.



6. Principes van de verwerking

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De Westerkim onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag

Persoonsgegevens worden door De Westerkim slechts in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Dit betekent onder meer dat verwerkingen slechts plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij De Westerkim voort uit een (zorg)overeenkomst, wet (wettelijke verplichting) of toestemming.

Welbepaalde doeleinden

De Westerkim verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat De Westerkim alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De Westerkim ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken, en De Westerkim van de verwerking afziet indien hetzelfde doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door het anonimiseren of aggregeren van gegevens.

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze persoonsgegevens in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De Westerkim voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest De Westerkim bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een voor de betrokkene minder inbreukmakende wijze kan worden verwezenlijkt dan kiest De Westerkim bij voorkeur voor die mogelijkheid.



Juiste en actuele gegevens

De Westerkim zorgt ervoor dat alleen persoonsgegevens worden verwerkt die accuraat, toereikend, ter zake dienend en niet bovenmatig zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De Westerkim neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd

De Westerkim stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en nodig voor het doel. Alleen als de bewaartermijn niet op basis van wettelijke bepalingen kan worden vastgesteld, stelt De Westerkim de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De Westerkim bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

De Westerkim neemt passende technische en organisatorische maatregelen om de Persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De Westerkim handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht De Westerkim om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

PRIVACY BY DEFAULT EN PRIVACY BY DESIGN

De Westerkim houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt *privacy by design* (PbD) genoemd. De Westerkim draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt De Westerkim *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

TOEGANG TOT GEGEVENS

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen De Westerkim geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De Westerkim hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het



bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

INBREUK IN VERBAND MET PERSOONSgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij De Westerkim, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De Westerkim registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken.

Samenwerking

De Westerkim schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving. De AVG verplicht De Westerkim tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten. Verder kan het voorkomen dat De Westerkim samenwerkt met andere (zorg)organisaties. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De Westerkim maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van De Westerkim.

DOORGIFTE BUITEN DE EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie

De Westerkim informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt De Westerkim van deze informatieplicht af.

RECHTEN VAN BETROKKENEN

Iedereen heeft het recht om te vernemen welke persoonsgegevens De Westerkim over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking



en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

GESCHILLENBESLECHTING

Indien de betrokkene van mening is dat De Westerkim niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

Onder de verantwoordelijkheid van de Raad van Bestuur vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt De Westerkim over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De Westerkim stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

VERWERKINGSREGISTER

De Westerkim beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

GEGEVENSEFFECTBEOORDELING (GEB)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet De Westerkim een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De Westerkim voert in dat geval een geveffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd). Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet DE WESTERKIM voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet De Westerkim met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

FUNCTIONARIS GEGEVENSBECHERMING (FG)

De Westerkim is een zorginstelling die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De Westerkim is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de Raad van Bestuur van zijn werkzaamheden, bevindingen en aanbevelingen.



PDCA CYCLUS

De Westerkim streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat De Westerkim weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Daarnaast gebruikt De Westerkim het NOREA Privacy Framework als borgingsproduct en als het beoordelingskader voor het waarborgen van privacy compliance binnen De Westerkim. Het NOREA Privacy Framework geeft invulling aan het normenkader voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen De Westerkim.

BEWUSTWORDING

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn binnen De Westerkim voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van waarbinnen die worden verwerkt.

7. Rollen en verantwoordelijkheden

Het privacy governance model van De Westerkim biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van de Raad van Bestuur, het management en medewerkers en de Functionaris voor de Gegevensbescherming (FG) en de ISO.

Privacy governance De Westerkim op hoofdlijnen

Verantwoordelijk	
Responsible/ Feitelijk verantwoordelijk	- Leidinggevend kader - De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
Accountable/ Eindverantwoordelijk	Raad van Bestuur
Consulted/ Adviserend	- Privacy Officer (indien aanwezig) - CISO/ISO (indien aanwezig) - Functionaris Gegevensbescherming



Informerend/ Geïnformeerd	• OR • Clientenraad • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)
------------------------------	--

Rollen en verantwoordelijkheden

RAAD VAN BESTUUR

De Raad van Bestuur is eindverantwoordelijk voor de naleving van de privacywetgeving binnen De Westerkim. De Raad van Bestuur heeft de volgende rollen en verantwoordelijkheden:

Eindverantwoordelijk voor de naleving van de de privacywetgeving binnen De Westerkim;

- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

LEIDINGGEVEND KADER

Het leidinggevend kader is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid. Zij hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevordert duurzame privacycultuur;
- Betrekt de FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.



FUNCTIONARIS VOOR GEGEVENSBESCHERMING (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor De Westerkim. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van De Westerkim:

- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen De Westerkim en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen;
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan de Raad van Bestuur;
- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van Data Protection Impact Assessments (DPIA's) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;



- Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over privacy-by-design bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

ANDERE ROLLEN EN VERANTWOORDELIJKHEDEN

Afdeling	Betrokkenheid
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)
Audit /Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).

8. Overlegstructuur

Binnen De Westerkim fungeert een werkgroep IB&P (Informatiebeveiliging en Privacy) die periodiek overlegt aangaande het thema informatieveiligheid en privacy. Aan dit overleg wordt deelgenomen door de controller/HEAD, ICT-beheerder, FG en bestuurssecretaris. Er wordt een actie en besluitenlijst gemaakt en gedocumenteerd.