Privacybeleid

Vierstroom Zorg Thuis

Eigenaar: Manager backoffice	**Vastgesteld door MT Vierstroom Zorg Thuis**
	Vaststellingsdatum: 19-03-2018
Versie: 13-03-2018, v10	**Evaluatiedatum:** 19-03-2019

Inhoudsopgave

1. Inleiding ... 3
Definities ... 4
Reikwijdte en doelstelling van het Beleid ... 5
Ingangsdatum en herziening ... 6
Beleidsuitgangspunt en -principes ... 7
3. Rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens ... 9
Raad van Bestuur (RvB) ... 9
Directie ... 9
Leidinggevende ... 9
Functionaris Gegevensbescherming ... 10
4. Implementatie Beleid ... 11
Bewustwording en training ... 11
Controle en naleving ... 11
Grondslag, doelbinding en belangenafweging ... 12
Vooronderzoek en documenteren van Verwerkingen ... 12
De organisatie van de beveiliging ... 12
Geheimhouding ... 12
Bewaartermijnen per soort Persoonsgegeven ... 12
Bijzondere Persoonsgegevens ... 13
Doorgifte persoonsgegevens aan derden ... 13
i. Uitbesteden van Verwerking aan een Verwerker ... 13
ii. Doorgifte Persoonsgegevens binnen de Europese Unie ... 13
iii. Doorgifte Persoonsgegevens buiten de Europese Unie ... 13
6. Incidenten met betrekking tot Persoonsgegevens (Datalek) ... 14
Melding en registratie ... 14
Evaluatie ... 14
Transparantie ... 16
Verzoek tot toegang tot, rectificatie van of wissen van Persoonsgegevens betreffende de Betrokkene ... 16
Termijn voor reageren op verzoeken van betrokkenen ... 16
Kennisgeving ... 16
Termijn voor uitvoering van verzoek ... 16
Recht van verzet ... 16
Rechtsbescherming ... 17
Mededeling van aanpassingen aan het Privacy Beleid ... 17

1. Inleiding

Vierstroom Zorg Thuis heeft als kernactiviteit het verlenen zorg in brede zin van het woord. De visie van Vierstroom Zorg Thuis is zich te concentreren op deze kerntaak en zo min mogelijk andere activiteiten te ontwikkelen. De focus is de uitvoering van de primaire zorgtaak.

Het verwerken van (bijzondere) persoonsgegevens is onlosmakelijk verbonden met het verlenen van zorg. Het niet beschikbaar zijn van gegevens of onjuiste gegevens kunnen verstrekkende gevolgen hebben voor het succes van de zorg en daarmee de gezondheid van cliënten. Misbruik van Persoonsgegevens kan tot grote schade leiden aan een organisatie, haar cliënten, haar medewerkers en andere betrokkenen zoals bijvoorbeeld leveranciers. Verwerking van Persoonsgegevens dient om deze redenen met de grootste zorgvuldigheid te gebeuren. Te weinig beveiliging is onacceptabel, tegelijkertijd mogen er geen onnodige hindernissen worden opgeworpen voor de medewerkers die de gegevens nodig hebben bij de uitvoering van hun primaire taken.

Doelstelling van Vierstroom Zorg Thuis is daarom te komen tot een optimale verhouding tussen genomen beveiligingsmaatregelen en toegankelijkheid van persoonsgegevens welke noodzakelijk zijn bij het verlenen van zorg en ondersteunende processen. Uiteraard is hierbij wet- en regelgeving richtinggevend.

Definities

i. Autoriteit Persoonsgegevens (AP): De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.
ii. Beleid: dit privacy beleid met betrekking tot het verwerken van persoonsgegevens binnen Vierstroom Zorg Thuis.
iii. Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie een persoonsgegeven betrekking heeft.
iv. Curator: Als toestemming de grondslag is voor een verwerking en de betrokkene is onder curatele gesteld, moet er expliciet toestemming aan de curator worden gevraagd. De curator is de belangenbehartiger en als zodanig benoemd door de kantonrechter.
v. Datalek: wanneer een onbevoegde inzage heeft gehad in Persoonsgegevens of als Persoonsgegevens per ongeluk zijn vernietigd of gewijzigd.
vi. Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
vii. Data Protection Impact Assessment (DPIA): een instrument waarmee vooraf de privacy risico's van gegevensverwerkingen in kaart worden gebracht. De DPIA wordt (verplicht) toegepast op verwerkingen welke waarschijnlijk een hoog privacy risico hebben. De DPIA is een belangrijk instrument om aan te tonen dat passende technische en organisatorische maatregelen zijn genomen.
viii. Functionaris Gegevensbescherming: De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp).
ix. Medewerker: persoon in loondienst van Vierstroom Zorg Thuis. Waar medewerker wordt genoemd, wordt naast de medewerker in loondienst, ook een ingehuurde medewerker (niet ZZP-er) en een vrijwilliger bedoeld.
x. Mentor: Als toestemming de grondslag is voor een verwerking en er sprake van mentorschap, dan moet er expliciet toestemming aan de mentor worden gevraagd. De mentor is de belangenbehartiger en als zodanig benoemd door de kantonrechter.
xi. Minderjarige: Als toestemming de grondslag is voor een verwerking en er worden mogelijk persoonsgegevens van kinderen onder de zestien verwerkt bij het aanbieden van een dienst of product, moet er expliciet toestemming aan de ouder of verzorger worden gevraagd. Kinderen vanaf 16 jaar moeten zelf toestemming geven voor het verwerken persoonsgegevens (art. 8 AVG).
xii. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
xiii. Privacy by Default: het principe dat met de standaard instellingen van een programma, app, website, dienst of apparaat de best passende privacy waarborging wordt gerealiseerd.
xiv. Privacy by Design: het al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) nadenken over en aandacht besteden aan een doelmatig gebruik van persoonsgegevens en de noodzaak om deze gegevens te gebruiken en te beschermen zoals onder andere het gebruik van privacy verhogende maatregelen en dataminimalisatie.
xv. Ontvanger: een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, waaraan persoonsgegevens worden verstrekt.
xvi. Samenwerkingsverband: samenwerking tussen organisaties kan noodzakelijk zijn om effectief zorg te kunnen verlenen. Bij het delen van persoonsgegevens moeten deelnemers aan het overleg voldoen aan de regels ter bescherming

van de privacy van betrokkenen. Alle betrokken organisaties moeten bevoegd zijn om deel te nemen aan het samenwerkingsverband.

xvii. Toestemming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling instemt met de verwerking van zijn of haar persoonsgegevens.

xviii. (Verwerkings-)verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

xix. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.

xx. Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde methodes, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Reikwijdte en doelstelling van het Beleid

Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Vierstroom Zorg Thuis waaronder in ieder geval alle (ex)-medewerkers, (ex)-cliënten, bezoekers, externe relaties etc., alsmede op andere betrokkenen waarvoor Vierstroom Zorg Thuis verantwoordelijke en/of verwerker is. Het begrip privacy moet hierbij breed opgevat worden en gaat zowel over geautomatiseerde verwerkingen als over fysieke dossiers maar is ook van belang in alle overige situaties waar persoonsgegevens aan de orde zijn.

Dit beleid is van toepassing op alle verwerkingen van persoonsgegeven welke plaatsvinden onder verantwoordelijkheid van Vierstroom Zorg Thuis. Het gaat hierbij zowel over persoonsgegevens welke zijn opgenomen in geautomatiseerde systemen als fysieke dossiers.

Het beschermen van persoonsgegevens heeft bij Vierstroom Zorg Thuis brede aandacht en staat in nauwe relatie met het Informatiebeveiligingsbeleid waarbij het gaat om de beschikbaarheid, de integriteit en de vertrouwelijkheid van data, waaronder ook persoonsgegevens.

Het beleid heeft als doel de kwaliteit van de verwerking en beveiliging van persoonsgegevens te optimaliseren waarbij privacy, functionaliteit en veiligheid en het leveren van zorg met elkaar in evenwicht zijn. Het doel is werk te kunnen uitvoeren zonder hinder van onnodige incidenten. Overmatige bureaucratie en ongebruiksvriendelijke beveiligingsmaatregelen dragen niet bij aan dit doel en kunnen contraproductief werken.

De doelstelling van het beleid van Vierstroom Zorg Thuis houdt concreet het volgende in:

i. Het bieden van een kader: het beleid biedt een kader om de (toekomstige) verwerking van persoonsgegevens te toetsen aan een vastgestelde ‘best practice’ norm. Tevens helpt dit kader om de taken, bevoegdheden en verantwoordelijkheden binnen Vierstroom Zorg Thuis te beleggen.

ii. Het stellen van normen: de basis voor de technische beveiliging van persoonsgegevens is het Informatiebeveiligingsbeleid van Vierstroom Zorg Thuis.

iii. Het nemen van de verantwoordelijkheid: door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor Vierstroom Zorg Thuis.

iv. Implementatie van het beleid te realiseren door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering en continue werking van de maatregelen.
v. Compliant zijn/worden met relevante wet- en regelgeving.
vi. Het creëren van bewustwording van het belang en de noodzaak van het beschermen van persoonsgegevens.
vii. Ter vermijding van (financiële) risico's als gevolg van het niet-compliant zijn met relevante wet- en regelgeving.
viii. Implementatie van / afstemming op bestaande Vierstroom Zorg Thuis protocollen zoals het Informatiebeveiligingsbeleid en het Protocol Beveiligingsincidenten en Datalekken.

Ingangsdatum en herziening

Dit privacy beleid van Vierstroom Zorg Thuis is goedgekeurd door S.J. Veenhoff, directeur van Vierstroom Zorg Thuis op 19-03-2018 en is geldig vanaf 25-05-2018. Dit beleid wordt periodiek geëvalueerd en zal waar nodig aangepast worden.

2. Beleidsprincipes Verwerking Persoonsgegevens

Beleidsuitgangspunt en -principes

Algemeen uitgangspunt van het beleid is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang en de noodzaak van Vierstroom Zorg Thuis om persoonsgegevens te verwerken en het belang (de rechten) van betrokkene om zijn of haar persoonlijke levenssfeer te beschermen.

Fundis Holding heeft de Interne Richtlijn; *WBP en de meldplicht Datalekken* uitgebracht welke als uitgangspunt voor de bedrijven in de Fundis vloot gehanteerd wordt.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

i. Verwerking van Persoonsgegevens vindt plaats op basis van één of meer rechtmatige grondslagen zoals genoemd in artikel 6 van de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679, hierna: “AVG”).
ii. Iedere verwerking wordt geregistreerd in een verwerkingsregister waarbij ten minste wordt vastgelegd:
    1. de naam en contactgegevens van de verantwoordelijke, eventuele gezamenlijke verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming (de FG);
    2. de doeleinden voor gegevensverwerking;
    3. een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens;
    4. de (voorgenomen) categorieën ontvangers;
    5. een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie;
    6. verwerkers van de gegevens;
    7. de (voorgenomen) bewaartermijnen en
    8. een algemene beschrijving van de beveiligingsmaatregelen.
iii. Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
iv. Bij een verwerking blijft de hoeveelheid en het soort gegevens beperkt tot die persoonsgegevens die noodzakelijk zijn voor het specifieke doel. Een belangrijk uitgangspunt van privacybescherming is dat zo min mogelijk persoonsgegevens worden verwerkt. Alleen die persoonsgegevens die nodig zijn om het doel te bereiken, mogen worden verwerkt. Het minimum aan persoonsgegevens is daarom ook meteen het maximum.
v. Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doel.
vi. Er worden maatregelen getroffen om zoveel mogelijk de actualiteit en juistheid van de te verwerken persoonsgegevens te waarborgen.
vii. Persoonsgegevens worden passend beveiligd en gebruikt zoals beschreven in het Informatiebeveiligingsbeleid.
viii. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
ix. Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
x. Iedere betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van zijn/haar persoonsgegevens, inclusief het recht van verzet.

xi. Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige zogenaamde opt-out procedure worden aangeboden.

In dit beleid wordt uitvoering gegeven aan de AVG en sectorale specifieke wetgeving zoals de WLZ, WGBO, Wet cliëntenrechten bij elektronische verwerking van gegevens, Wkkgz etc.

3. Rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens

Om de verwerking van persoonsgegevens gestructureerd en gecoördineerd te realiseren zijn binnen *Organisatie* de volgende rollen onderkend en toegewezen:

Raad van Bestuur (RvB)

Conform het Vlootmodel zijn de bedrijven verantwoordelijk voor de naleving van de Wbp (per mei 2018 AVG). In de Interne Richtlijn; *WBP en de meldplicht Datalekken* geeft de RvB duidelijk richting aan wat van de afzonderlijke bedrijven wordt verwacht. Over de invulling van de naleving van de Wbp geeft de RvB geen nadere richtlijnen. Hier zijn de directies van de bedrijven voor verantwoordelijk.

De afdeling Risk & Compliance is vanwege haar tweedelijns verantwoordelijk beschikbaar voor advies inzake diverse aspecten van de Wbp. Daarnaast zal zij vanuit een Risico en Compliance invalshoek er op toe zien dat de naleving van de Wbp en in het bijzonder de Meldplicht Datalekken voldoende geborgd zijn binnen de processen, de risicomatrices en de Interne beheersing binnen de bedrijven.

Directie

De bedrijven leggen periodiek verantwoording af aan de RvB over de naleving /niet naleving van de Wbp inclusief de Meldplicht Datalekken. Het is tevens de verantwoordelijkheid van de directieleden van de bedrijven om ernstige datalekken en overige inbreuken op de naleving van de Wbp met mogelijk aanzienlijke impact, aan de RvB te melden.

De afdeling Risk & Compliance legt als onderdeel van haar reguliere werkzaamheden periodiek verantwoording af aan de Holding Directie inzake de mate waarin de AO/IC's binnen de bedrijven in staat zijn om de risico's inzake de WBP en de Meldplicht Datalekken adequaat minimaliseren/beheersen.

De RvB beoordeelt periodiek de naleving van de WBP en de Meldplicht Datalekken.

De directie bepaalt doel en middelen van de verwerking en is daardoor aan te merken als de verantwoordelijke voor verwerkingen. De directie beoordeelt beveiligingsincidenten en neemt besluiten over het al dan niet te melden van datalekken bij de AP en het informeren van betrokkenen. Deze besluiten en de overwegingen op basis waarvan deze besluiten worden genomen, worden vastgelegd.

Leidinggevende

Het creëren van bewustwording en de naleving van het Beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

i. er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beleid;
ii. toe te zien op de naleving van het beleid door zijn medewerkers;
iii. periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen;
iv. een incident onverwijld te melden aan de directie.

Medewerker

Dit privacy beleid geldt voor alle medewerkers (ook uitzend- en inhuurkrachten) en voor vrijwilligers. Kortom allen die bij het uitvoeren van hun werkzaamheden te maken kunnen krijgen met het verwerken van persoonsgegevens of het delen van gevoelige persoonsgegevens. Medewerkers hebben een eigen verantwoordelijkheid, zijn verplicht zich te houden aan de verstrekte gedragscode aangaande de omgang met persoonsgegevens en dienen zich altijd bewust te zijn van hun bijzondere verantwoordelijkheid jegens cliënten. Ze dienen te handelen conform het beleid met als doel maximale bescherming van de persoonsgegevens. Daarnaast is de medewerker verplicht afwijkingen en misstanden te melden aan de leidinggevende en de sleutelfiguur privacy binnen de eigen organisatie.

Sleutelfiguur privacy/ contactpersoon

Elk bedrijf heeft een sleutelfiguur privacy aangewezen die ‘deskundige’ is voor de omgang met persoonsgegevens. Deze sleutelfiguur heeft de volgende taken:

I. Eerste aanspreekpunt binnen de eigen organisatie bij een incident;
II. Actief in het bevorderen van een juiste omgang met persoonsgegevens;
III. Eerste contactpersoon voor de FG;
IV. Beheerder van het verwerkingenregister.

Functionaris Gegevensbescherming

Bij het in werking treden van de AVG is de benoeming van een Functionaris Gegevensbescherming (FG) in sommige gevallen verplicht. De FG is een interne toezichthouder op de verwerking van persoonsgegevens. De FG houdt binnen het bedrijf toezicht op de toepassing en naleving van de AVG en adviseert de directie (gevraagd en ongevraagd) over onderwerpen omtrent de bescherming van persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie en de FG ontvangt dan ook geen aanwijzingen van de verantwoordelijke bij het uitoefenen van zijn taak.
De FG treedt op als contactpersoon van de Autoriteit Persoonsgegevens, als interne privacy auditor en als adviseur ten aanzien van privacy gerelateerde aangelegenheden. Vierstroom Zorg Thuis heeft gezamenlijk met andere Fundis-bedrijven een FG benoemd. De FG rapporteert aan de verantwoordelijke (directeur). Conform het vlootmodel kan de FG in uitzonderlijke gevallen genoodzaakt zijn om de RvB te informeren.

4. Implementatiebeleid

Dit privacy beleid is geen eenmalige activiteit, maar juist onderdeel van een continue proces van verfijning/aanpassing/verbetering. In deze context is de Plan-Do-Check-Act cyclus bij de bescherming van persoonsgegevens relevant.

Bewustwording en training

Beleid en maatregelen alleen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens zo klein mogelijk te maken. Noodzakelijk is om het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Hiertoe zijn regelmatig terugkerende trainingen en bewustwordingscampagnes voor medewerkers en overige groepen die bij de uitvoering van hun werkzaamheden te maken krijgen met privacygevoelige informatie noodzakelijk. Het verhogen van de veiligheids- en privacy bewustwording is vanuit de verantwoordelijke (directie) gedelegeerd aan het lijnmanagement. Bewustwording wordt tevens gerealiseerd door dit onderwerp aan de orde te stellen in reguliere overleggen zoals teamoverleg en functioneringsgesprekken.

De sleutelfiguur Privacy heeft als taak onwenselijke omgang met persoonsgegevens op de werkvloer te signaleren en hier aandacht voor te vragen bij het management.

Controle en naleving

Om het beleid en de genomen maatregelen te controleren op effectiviteit worden audits uitgevoerd conform de Richtlijn WBP en Wet Meldplicht Datalekken. De bedrijven leggen periodiek verantwoording af aan de Holding Directie over de naleving /niet naleving van de WBP en de Meldplicht Datalekken. De afdeling Risk & Compliance legt als onderdeel van haar reguliere werkzaamheden periodiek verantwoording af aan de Holding Directie inzake de mate waarin de AO/IC's binnen de bedrijven in staat zijn om de risico's inzake de Wbp en de Meldplicht Datalekken adequaat minimaliseren/beheersen. Eventuele externe controles worden uitgevoerd door onafhankelijke auditors of accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale planning & control cyclus. Het verwerken van persoonsgegevens is een continu proces. Indien de naleving op de bescherming van persoonsgegevens ernstig tekort schiet, kan het betreffende Fundis-bedrijf de betrokken verantwoordelijke medewerker(s) een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Evaluatie

Technologische en/of organisatorische ontwikkelingen binnen en buiten het eigen bedrijf maken het noodzakelijk om periodiek te bezien of het beleid nog voldoende kaders biedt of dat er aanpassingen noodzakelijk zijn. Het is de taak van leidinggevenden om hierop toe te zien en bij gewenste aanpassingen contact op te nemen met betrokkenen.

5. Rechtmatige en zorgvuldige verwerking van persoonsgegevens

Grondslag, doelbinding en belangenafweging

Het verwerken van persoonsgegevens moet gebaseerd zijn op één of meer rechtmatige grondslagen zoals beschreven in artikel 6 van de AVG. De verwerkingsverantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Dit wordt vastgelegd in een verwerkingenregister. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Bij projecten, IT-infrastructurele wijzigingen of de aanschaf van nieuwe (informatie)systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door het hanteren van de principes Privacy by Design en Privacy by Default. Tevens kan bij nieuwe projecten en/of changes een DPIA worden uitgevoerd. De DPIA geeft een indicatie van het risico van de voorgestelde verwerking en bijgevolg de relevante dataclassificatie en noodzakelijke beschermingsmaatregelen.

Vooronderzoek en documenteren van Verwerkingen

Iedere verwerking van persoonsgegevens dient te worden geregistreerd in een daartoe opgezet verwerkingsregister. De verantwoordelijke beoordeelt de grondslag van de verwerking en ziet toe op adequate registratie in het verwerkingenregister. Hij kan hierbij de hulp inroepen van de FG. In het geval van verwerking met een hoog risico voor de betrokkenen zoals bijvoorbeeld van bijzondere en/of gevoelige persoonsgegevens pleegt de verantwoordelijke altijd voorafgaande consultatie bij de FG.

De organisatie van de beveiliging

Organisatie draagt zorg voor een adequaat beveiligingsniveau en implementeert passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking en verlangt dit ook van derden die in haar opdracht persoonsgegevens verwerken. Gemaakte afspraken met verwerkers worden vastgelegd in een verwerkersovereenkomst. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen, te onderkennen en te corrigeren. Tevens hebben deze maatregelen betrekking op de wijze van beveiliging door de verwerker.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het interne risicobeheersings- en controlesysteem van het betreffende bedrijf.

Geheimhouding

Vierstroom Zorg Thuis classificeert de vertrouwelijkheid van alle persoonsgegevens. Een ieder behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen. Ook personen voor wie niet reeds uit hoofde van een ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen. Geheimhouding is als onderwerp opgenomen in het arbeidscontract van de werknemer en het inhuurcontract en overeenkomst met ingezette ZZP-ers. Alle interne/externe medewerkers die toegang hebben tot vertrouwelijke informatie zijn aan geheimhouding gebonden. In de overeenkomsten met verwerkers is opgenomen dat medewerkers van de verwerkende organisatie verplicht zijn persoonsgegevens geheim te houden.

Bewaartermijnen per soort persoonsgegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Medische of zorginhoudelijke persoonsgegevens worden dienen na beëindiging van de behandeling of verpleging buiten het

bereik van de actieve administratie gebracht. Persoonsgegevens worden door Vierstroom Zorg Thuis na het verlopen van de geldende bewaartermijn vernietigd.

Bijzondere persoonsgegevens

Het verwerken van bijzondere en gevoelige persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend (algemeen) belang. Tevens gelden ten aanzien van deze persoonsgegevens zwaardere beveiligingseisen, afhankelijk van het resultaat van de DPIA. Onder bijzondere en gevoelige persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond, strafrechtelijke gegevens maar ook BSN, kopie ID-bewijs en pasfoto.

Doorgifte persoonsgegevens aan derden

i. Uitbesteden van verwerking aan een verwerker
   Indien verantwoordelijke persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van de verwerkingen geregeld in een schriftelijke overeenkomst tussen verantwoordelijke en de verwerker; de verwerkersovereenkomst.
ii. Doorgifte persoonsgegevens binnen de Europese Unie
   Verantwoordelijke verstrekt persoonsgegevens aan derden binnen de Europese Unie slechts op basis van één of meer rechtmatige grondslagen zoals beschreven in artikel 6 van de AVG. Bijzondere persoonsgegevens worden niet aan derden verstrekt zonder expliciete toestemming van de betrokkene, tenzij het een wettelijke verplichting betreft. Betrokkene wordt hierover altijd geïnformeerd.
iii. Doorgifte persoonsgegevens buiten de Europese Unie
   Verantwoordelijke verstrekt persoonsgegevens alleen aan derde partijen die zich bevinden in een land buiten de Europese Unie nadat de regelgeving hieromtrent geraadpleegd is en aan de regels die hiervoor gelden is voldaan. Dit is in dit beleid niet nader uitgewerkt aangezien de kans dat dit zich zal voordoen minimaal wordt geacht.

6. Incidenten met betrekking tot persoonsgegevens (datalek)

Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen Vierstroom Zorg Thuis wordt beschouwd als een privacy gerelateerd incident. De bekendste vorm van zo'n incident is een datalek.

Melding en registratie

Datalekken en incidenten die als datalek zouden kunnen worden aangemerkt, dienen zo spoedig mogelijk, doch uiterlijk binnen 4 uur na ontdekking, te worden gemeld bij het sleutelfiguur Privacy en de leidinggevende, ook buiten kantoortijden en op zon- en feestdagen. Dit kan via e-mail of telefonisch. Elk gemeld incident en de afhandeling daarvan wordt geregistreerd. Een incident kan ook worden gemeld door een betrokkene, verwerker of door een derde persoon. Met een verwerker dienen afspraken te worden gemaakt over het melden van een incident met persoonsgegevens.

Afhandeling

Nadat een incident is gemeld neemt de ontvanger van de melding contact op met de melder om de melding door te nemen. Indien nodig wordt de FG betrokken bij de afhandeling. Sleutelfiguur en FG bepalen of er sprake is van een datalek en schrijven een advies aan de verantwoordelijke met het verzoek om besluitvorming omtrent de verdere afhandeling van het datalek (wel of niet melden bij de AP en aan betrokkene(n)).

De FG kan besluiten een commissie Datalekken aan te wijzen. Deze commissie heeft de taak een verdergaand onderzoek te doen naar de toedracht van het datalek. Deze commissie evalueert het advies en de afhandeling van het lek en stelt verbetervoorstellen vast om nieuwe datalekken te voorkomen. De commissie zal in ieder geval rapporteren aan de betreffende bestuurder en zal de sleutelpersoon bij het onderzoek betrekken. De FG is altijd lid van de commissie Datalekken.

Indien noodzakelijk doet de sleutelfiguur binnen 72 uur na ontdekking van het datalek, melding bij de AP en/of de betrokkene(n).

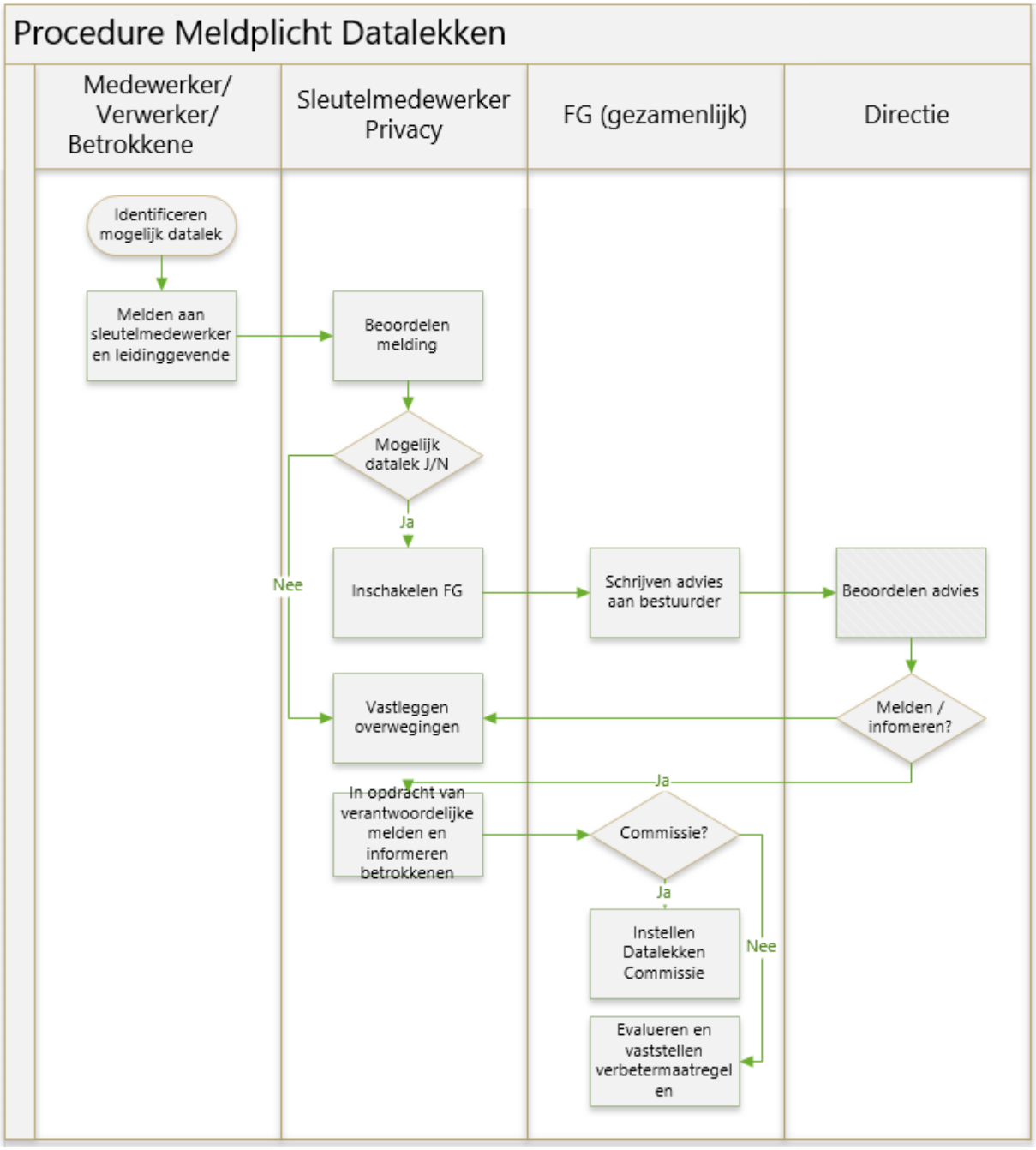
Evaluatie

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De sleutelfiguren rapporteren maandelijks aan de FG. De rapportage over incidenten met betrekking tot persoonsgegevens maken als vast onderdeel de jaarrapportage van RvB. De FG levert hier input voor in een rapportage aan de RvB.

Procedure Meldplicht Datalekken

Voor de juiste afhandeling van een beveiligingsincident met betrekking tot persoonsgegevens is een procedure vastgesteld. In deze procedure is de verantwoordelijkheid van elke betrokkene vastgelegd. Hiermee worden taken en verwachtingen duidelijk gemaakt.

Hieronder is deze procedure schematisch weergegeven:


Procedure Meldplicht Datalekken
Medewerker/ Verwerker/ Betrokkene
Sleutelmedewerker Privacy
FG (gezamenlijk)
Directie
Identificeren mogelijk datalek
Melden aan sleutelmedewerker en leidinggevende
Beoordelen melding
Mogelijk datalek J/N
Ja
Nee
Inschakelen FG
Schrijven advies aan bestuurder
Beoordelen advies
Melden / infomeren?
Vastleggen overwegingen
Ja
In opdracht van verantwoordelijke melden en informeren betrokkenen
Commissie?
Ja
Nee
Instellen Datalekken Commissie
Evalueren en vaststellen verbetermaatregelen

7. Rechten van betrokkenen

Transparantie

Vierstroom Zorg Thuis faciliteert de uitoefening van de rechten van betrokkene uit hoofde van de AVG en informeert de betrokkene op een eenvoudig toegankelijke en begrijpelijke manier. Het gaat hierbij specifiek over:

i. De identiteit en contactgegevens van de voor de verwerking verantwoordelijke.
ii. De specifieke doeleinden van de Verwerking waarvoor de persoonsgegevens zijn bestemd alsook informatie betreffende de hoeveelheid, de bewaartermijn van de gegevens en de maatregelen die zijn genomen om de persoonsgegevens te beschermen.

Verzoek tot toegang tot, rectificatie van of wissen van persoonsgegevens betreffende de betrokkene

Iedere betrokkene kan, met betrekking tot over hem opgenomen persoonsgegevens, bij Vierstroom Zorg Thuis een verzoek indienen om toegang te krijgen tot die persoonsgegevens, die te wijzigen, verbeteren, aan te vullen, te verwijderen of af te schermen. Een verzoek tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens van minderjarigen die de leeftijd van 16 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger. Dit geldt ook voor personen die onbekwaam zijn en een door de kantonrechter benoemde mentor of curator vertegenwoordigd worden. Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige zogenaamde opt-out procedure worden aangeboden.

Termijn voor reageren op verzoeken van betrokkenen

Vierstroom Zorg Thuis geeft zo snel mogelijke maar in ieder geval binnen een maand na ontvangst invulling aan het verzoek van betrokkene.

Kennisgeving

Vierstroom Zorg Thuis zorgt voor correctie van persoonsgegevens welke feitelijk onjuist zijn, voor het doel of doeleinden van de verwerking onvolledig of niet ter zake doen of in strijd met een wettelijk voorschrift zijn verwerkt. Vierstroom Zorg Thuis informeert derden aan wie de persoonsgegevens zijn verstrekt en ziet er op betreffende persoonsgegevens worden gecorrigeerd. De verzoeker mag opgave verzoeken van degene aan wie Vierstroom Zorg Thuis deze mededeling heeft gedaan.

Termijn voor uitvoering van verzoek

De organisatie zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens zo spoedig mogelijk wordt uitgevoerd.

Recht van verzet

i. <u>Gronden voor verzet</u>
   In verband met zijn of haar specifieke persoonlijke omstandigheden, mag iedere betrokkene verzet aantekenen tegen verwerking van zijn/haar persoonsgegevens door Vierstroom Zorg Thuis, als deze verwerking plaatsvond op grond van:
   1. de vervulling van een publiekrechtelijke taak van de verwerkingsverantwoordelijke.
   2. de behartiging van het gerechtvaardigd belang van Vierstroom Zorg Thuis of van een derde aan wie de persoonsgegevens worden verstrekt.

ii. <u>Termijn</u>
   Vierstroom Zorg Thuis beoordeelt binnen vier weken na ontvangst van het verzet of deze gerechtvaardigd is. Indien het verzet gerechtvaardigd is, treft Vierstroom Zorg Thuis maatregelen die nodig zijn om de verwerking de beëindigen.

Rechtsbescherming

Bij klachten over de verwerking van persoonsgegevens kunnen betrokkenen dit in eerste instantie aan de betreffende medewerker(s) of leidinggevende van de medewerker(s) melden. Zij behandelen deze klacht als een mogelijk incident en volgen de procedure Meldplicht Datalekken.

Ook is het mogelijk dat de klachtenfunctionaris wordt benaderd. Deze is geïnformeerd hoe te handelen en neemt contact op met de sleutelfiguur Privacy van Vierstroom Zorg Thuis.

Mededeling van aanpassingen aan het Privacy Beleid

Als het beleid mettertijd ingrijpend wordt aangepast dan wel veranderd, deelt Vierstroom Zorg Thuis deze algemeen mee, om een zorgvuldige en behoorlijke verwerking van de persoonsgegevens te waarborgen.