Verantwoordingsverklaring inzake gegevensbescherming 2021

Verantwoording van Orpea in Nederland aan betrokkenen over het voldoen aan wet- en regelgeving op het gebied van bescherming van persoonsgegevens

Woonzorg

BLOEMENDAEL
WOON- EN ZORGVOORZIENING

COMPARTIJN

september

Van Hollant
VERZORGD WONEN, VRIJ LEVEN

Thuiszorg

ALLERZORG

GGZ

WOONZORGNET

ZORGVERLENING
PGZ

't Zicht zorggroep

Juni 2022

Inhoudsopgave

1. Inleiding

1.1. Doel verklaring

Dagelijks ontvangen onze bewoners en cliënten zorg van onze zorgverleners. Hiervoor is het noodzakelijk dat onze zorg- en hulpverleners op de hoogte zijn van de gezondheidstoestand van de cliënten en weten waarmee zij in het kader van de hulp- en zorgverlening rekening moeten houden. Daarnaast hebben we ook gegevens van onze bewoners, cliënten en medewerkers nodig voor administratieve taken zoals het declareren van zorg en het betalen van salarissen.

De persoonsgegevens die hiervoor worden verwerkt zijn het eigendom van degenen op wie deze gegevens betrekking hebben, de betrokkenen. Zonder deze gegevens kan geen zorg geleverd worden. De betrokkenen verstrekken ons hun gegevens in het vertrouwen dat deze op een integere, juiste en vertrouwelijk wijze worden verwerkt.

Met deze verklaring leggen de bedrijven van Orpea in Nederland (hierna 'Orpea') verantwoording af aan alle belanghebbenden over de naleving van de wettelijke verplichtingen op het gebied van gegevensbescherming. Dit gebeurt op basis van wat is vastgelegd en gedocumenteerd en waarmee de effectieve werking van de technische en organisatorische maatregelen worden aangetoond. Daarmee wordt beoogd dat het vertrouwen wat de betrokken in ons stellen, wordt bevestigd.

1.2. Gebruik van de verklaring

Deze verklaring is onderdeel van de governance en compliance van Orpea en is als volgt vormgegeven. De Raad van Bestuur heeft beleid vastgesteld op basis van het advies van de functionaris gegevensbescherming (FG). Aan de hand daarvan zijn de processen en systemen ingericht. De eigenaren van deze processen en systemen zijn verantwoordelijk voor het inrichten van technische en organisatorische beveiligingsmaatregelen. Zij zorgen voor een continue effectieve werking en maken dit aantoonbaar. Hierbij worden zij ondersteund door de informatiemanager (verschaft techniek), de FG (adviseert o.g.v. wetgeving en de praktijk), de ISO (adviseert ten aanzien van informatiebeveiliging).

De FG verzamelt de vastgelegde gegevens en documentatie informatie met betrekking tot het aantonen dat en in hoeverre aan de wettelijke verplichtingen wordt voldaan. Op basis daarvan is deze verantwoordingsverklaring opgesteld. De verklaring is bestemd voor de stakeholders waaronder betrokkenen, leveranciers, financiers en toezichthouders. De controle op (aspecten) van gegevensbescherming is onderdeel van de controle op de jaarrekening door de externe accountant. De externe accountant kan de inhoud van deze verklaring betrekken bij het vaststellen van zijn controleverklaring.

Door middel van de 'Mededeling Raad van Bestuur' legt de Raad verantwoording af als verwerkingsverantwoordelijke over de verwerking van persoonsgegevens in 2021. De FG licht in de 'Mededeling functionaris voor gegevensbescherming' toe welke rol deze heeft gehad met betrekking tot zijn wettelijke taken.

1.3. Afkortingen

In deze verantwoordingsverklaring worden een aantal afkortingen gebruikt. In onderstaande tabel worden deze afkortingen verklaard.

Afkorting/term	Betekenis
AVG	Algemene Verordening Gegevensbescherming, Europese wetgeving op het gebied van de bescherming van persoonsgegevens.
DPIA	Data Protection Impact Assessment, gestructureerde inventarisatie van risico's die een verwerking voor betrokkenen heeft.
ECD	Elektronisch cliënten dossier, dossier waarin alle gegevens van de bewoner/cliënt zijn opgeslagen.
FG	Functionaris gegevensbescherming, intern toezichthouder en adviseur op het gebied van gegevensbescherming.
GGZ	Geestelijke gezondheidszorg
HRM	Human Resource Management
ICT	Informatie en communicatie technologie
ISO	Information security officer, specialist op het gebied van informatiebeveiliging.
PTZ	Palliatief terminale zorg
Wkkgz	Wet kwaliteit, klachten en geschillen zorg

2. Mededeling Raad van Bestuur

Net als in 2020 is COVID-19 van invloed geweest op de dagelijkse gang van zaken. In het tweede jaar van de pandemie heeft de organisatie geleerd om te gaan met de effecten van het virus. Dit geldt ook voor de vraagstukken op het gebied van privacy en gegevensbescherming in relatie met de coronamaatregelen. Wij hebben de draad weer opgepakt en onze focus gericht op de hulp- en zorgverlening van onze bewoners en cliënten.

In 2021 zijn nieuwe bedrijven aan de groep van Orpea toegevoegd. In januari is Van Hollant Heiloo BV overgenomen door September Holding BV. Van Hollant biedt kleinschalige woonzorg aan in Noord Holland voor dementerende ouderen. In maart is Zorggroep ’t zicht overgenomen door Woonzorgnet BV. Zorggroep ’t Zicht heeft in Zuidoost Nederland een aantal GGZ-locaties voor meer- en minderjarigen met een psychische hulpvraag. In april is PGZ overgenomen door Allerzorg. PGZ is een specialist op het gebied van autisme in Zuid Nederland en biedt naar een aantal woonlocaties ook ambulante begeleiding.

De integratie van de overgenomen bedrijven in de Orpea organisatie wordt begeleid door een integratieteam. Hierbij is aandacht voor de verwerking van persoonsgegevens. De FG wordt periodiek geïnformeerd over de voortgang en status van de integratie en heeft op het gebied van naleving van wet- en regelgeving een actieve rol.

Orpea werkt samen met andere zorgaanbieders om goed aan te sluiten op de zorgvraag vanuit de markt en om de zorg betaalbaar te houden. Om te waarborgen dat deze samenwerking binnen de kaders van de AVG plaatsvindt, wordt de FG bij de totstandkoming van de samenwerking betrokken. Een voorbeeld is de samenwerking met iCare ten behoeve van de ongeplande nachtzorg in de regio Flevoland. Omdat hierbij persoonsgegevens met een andere zorgaanbieder worden uitgewisseld is door de samenwerkende partijen een gezamenlijke DPIA uitgevoerd en zijn maatregelen getroffen om de risico’s op het gebied van gegevensbescherming voor de betrokkenen te minimaliseren.

Binnen Orpea zijn in 2021 30 datalekken intern bij de FG gemeld. Elk datalek is door de FG onderzocht en naar aanleiding daarvan zijn zestien datalekken bij de Autoriteit Persoonsgegevens gemeld omdat sprake was van een risico voor de betrokkenen. Daarbij zijn ook de betrokkenen van het datalek op de hoogte gesteld. In de meeste gevallen was sprake van het verkeerd verzenden van gegevens via post of e-mail. De betrokken bedrijven hebben naar aanleiding van de datalekken maatregelen getroffen om deze datalekken zoveel mogelijk te voorkomen.

In 2021 is aandacht geweest voor de bewustwording van medewerkers ten aanzien van de verwerking van persoonsgegevens. Hiervoor zijn online themaweken georganiseerd waar medewerkers aan hebben kunnen deelnemen. Ook zijn regelmatig artikelen gepubliceerd over privacy en gegevensbescherming en is tweemaal een masterclass gegeven omtrent dit onderwerp.

Voor 2022 geldt dat we verder inzetten op de bewustwording van de medewerkers. Zij zijn immers een belangrijke schakel in de verwerking van de persoonsgegevens. Het aantal uit te voeren DPIA’s wordt in 2022 opgevoerd zodat maatregelen worden getroffen om de betrokkenen zoveel mogelijk te beschermen. Samen met de FG worden de ontwikkelingen op het gebied van privacy en gegevensbescherming gevolgd zodat Orpea kan aantonen dat aan de wettelijke verplichtingen wordt voldaan.

Roy Rempe,	Geert Uytterschaut
Bestuurder	Bestuurder

3. Mededeling functionaris gegevensbescherming

3.1. Ontwikkelingen

De organisatie is ook in 2021 in beweging geweest. De samenwerking tussen de bedrijven van Orpea in Nederland wordt steeds hechter. Dit heeft voordelen op het gebied van kennisdeling en schaalvergroting. Het kent ook aandachtspunten ten aanzien van de verwerking van persoonsgegevens. Het gaat dan bijvoorbeeld over het delen en bewaren van persoonsgegevens en het gebruik van brongegevens en duplicaten.

3.2. Positie en deskundigheid

Van de FG wordt verwacht dat deze onafhankelijk, onpartijdig en integer opereert. Deze eigenschappen van de rol en positie van de FG zijn wettelijk verankerd. Als FG hanteer ik deze bij de in vulling van mijn taken en positie binnen de organisatie. In een driemaandelijks bestuurlijk overleg rapporteer ik over de uitvoering van het gegevensbeschermingsbeleid rechtstreeks aan de Raad van Bestuur.

De groei van de organisatie heeft onder andere tot gevolg dat de vraagstukken op het gebied van privacy en gegevensbescherming meer en meer juridisch componenten bevatten. Om die reden heb ik in 2021 een module van de bachelor studie Rechtswetenschappen van de Open Universiteit afgerond. Om op de hoogte te blijven van de wettelijke, technische en maatschappelijke ontwikkelingen op het gebied van gegevensbescherming worden deze onderwerpen in een maandelijkse studieochtend bestudeerd. Daarnaast ben ik als FG lid van een aantal werkgroepen en netwerken. En als het weer kan, worden bijeenkomsten en congressen bezocht. Hiermee wordt voldaan aan de wettelijke vereiste dat de FG beschikt over voldoende deskundigheid en competenties om zijn rol goed te vervullen.

3.3. Rol

De rol van de FG raakt steeds meer ingebed in de organisatie en blijft zich ontwikkelen zoals ook de organisatie blijft ontwikkelen. In 2021 en voorgaande jaren heb ik ingezet om de organisatie zoveel mogelijk te informeren en te adviseren over de naleving van de AVG en de wet- en regelgeving die de verwerking van persoonsgegevens raakt.

Dit zal ik ook in 2022 blijven doen en vanwege de volwassenheid van de organisatie zal mijn rol een meer toezichthoudende en ondersteunend karakter krijgen. Het doel is om degenen die binnen de organisatie feitelijke invloed uitoefenen op het te voeren beleid en de verwerking van persoonsgegevens te ondersteunen bij de uitoefening van diens taken op dit gebied. Maar ook om informatie te verzamelen waarbij verantwoording over naleving van wet- en regelgeving wordt afgelegd.

Frans Schreuder

Functionaris Gegevensbescherming

4. Organisatiebeschrijving

4.1. Algemeen

Orpea is een internationale en beursgenoteerde onderneming die binnen en buiten Europa opereert als zorgaanbieder. Een aantal zorgbedrijven opereert onder de vlag van Orpea in Nederland. Deze verantwoordingsverklaring is van toepassing op de bedrijven die in Figuur 1 staan. Binnen Orpea werken deze bedrijven op internationaal vlak samen waarbij kennis en ervaring onderling worden uitgewisseld. Binnen Europa zijn de bedrijven in Nederland onderdeel van het Cluster Noord Europa dat verder bestaat uit de zorgbedrijven in België, Luxemburg, het Verenigd Koninkrijk en Ierland. Binnen Orpea wordt op verschillend niveau maandelijks overleg gevoerd over gegevensbescherming en de daaraan verbonden documentatie, processen en vraagstukken.

4.2. Pijlerstructuur

De organisatie is in een pijlerstructuur opgedeeld: Woonzorg, GGz en Thuiszorg. De organisatie wordt ondersteund door een servicebureau. Hier worden de bulkprocessen uitgevoerd zoals de personeels- en salarisadministratie, financiële administratie, kwaliteitsmanagement en ICT.

Binnen deze pijlerstructuur zijn vier bedrijven te onderscheiden die – op grond van de huidige juridische structuur – het doel en middelen van de verwerking vaststellen en daarmee verwerkingsverantwoordelijken zijn. Dit zijn:

- Allerzorg Beheer BV (inclusief Allerzorg BV, Allerzorg Support BV, PGZ Groep BV en Zorgverlening PGZ BV)
- Compartijn Holding BV (inclusief Compartijn Exploitatie BV)
- September Holding BV (inclusief Wonen bij September BV, BLMDL BV en Van Holland Heiloo BV)
- Woonzorgnet BV (inclusief Zorggroep ’t Zicht BV)

Figuur 1

5. Verwerking van persoonsgegevens

5.1. Beleid

Orpea voert een gegevensbeschermingsbeleid met als doel de wettelijke vereisten die op de verwerking van persoonsgegevens rusten concreet te vertalen naar de uitvoering. In het beleid wordt uitgegaan van tien principes die op de verwerking van persoonsgegevens van toepassing zijn. Deze principes worden op verschillend niveau gebruikt in gerelateerde beleidsdocumenten, processen en instructies. Ook wordt hierover met de medewerkers gecommuniceerd. Hiervoor is een speciale 'privacypagina' op SharePoint ingericht die voor elke medewerker gemakkelijk toegankelijk is.

5.2. Gerechtvaardigde doeleinden

De persoonsgegevens worden verwerkt met als doel het verlenen van gezondheidszorg aan cliënten thuis in de vorm van verpleging en verzorging, begeleiding en behandeling. Alle overige verwerkingen van persoonsgegevens, zoals die van medewerkers zijn gerelateerd en afgeleid van dit doeleinde. Op het verwerken van bijzondere categorieën persoonsgegevens, zoals gezondheidsgegevens rust een wettelijk verbod. Hierop is het verlenen van gezondheidszorg een wettelijke uitzondering. Orpea is een zorgaanbieder en voldoet daarmee aan deze uitzonderingssituatie.

5.3. Rechtmatigheid

De verwerkingen van persoonsgegevens rusten op een geldige rechtsgrond. In de meeste gevallen is de verwerking van persoonsgegevens noodzakelijk voor de uitvoering van de overeenkomst waarbij de betrokkene partij is. Hiermee wordt bedoeld de (woon-)zorgovereenkomst met de cliënt/bewoner of de arbeidsovereenkomst met de werknemer. De rechtsgrond van een aantal verwerkingen rust op de noodzaak om aan een wettelijke verplichting te voldoen zoals bijvoorbeeld aan de belastingwetgeving en de wetgeving die van toepassing op het verlenen van gezondheidszorg zoals de Wkkgz.

In een beperkt aantal gevallen rust de verwerking op de grondslag 'gerechtvaardigd belang', waarbij de belangen van de betrokkenen zijn afgewogen met de belangen van Allerzorg. Dit is bijvoorbeeld noodzakelijk voor het beheren en onderhouden van de digitale infrastructuur en applicaties. In dat geval zijn de belangen van de betrokkenen zorgvuldig afgewogen tegenover de belangen van de betrokkenen.

5.4. Juistheid

Voor een veilige en verantwoorde zorgverlening aan cliënten is het van groot belang dat de gegevens van cliënten juist, volledig en actueel zijn. Ook is het van groot belang dat de gegevens betrekking hebben op de juiste persoon. Om te waarborgen dat aan deze eisen wordt voldaan, maakt Orpea gebruik van verschillende ECD's. Hierin worden de persoonsgegevens op cliëntniveau gebundeld en gestructureerd. De primaire processen zijn gebaseerd op de gegevens vanuit de ECD's. Via regelmatige kwaliteitscontroles wordt vastgesteld of de persoonsgegevens in de ECD's juist, volledig en actueel zijn. Voor 2022 wordt ingezet op een vereenvoudiging van het applicatielandschap waardoor Orpea van een uniform ECD gebruik zal gaan maken.

Voor een juiste uitvoering van de arbeidsovereenkomst en de wettelijke verplichtingen die hierop rusten is het eveneens belangrijk dat de persoonsgegevens van werknemers juist, volledig en actueel zijn. Om deze reden worden deze persoonsgegevens eveneens in een digitaal dossier verwerkt. Bij de instroom van nieuwe medewerkers worden de actuele persoonsgegevens opgevraagd en verwerkt.

Er zijn diverse controles op de echtheid van het identiteitsbewijs en de aangeleverde diploma's. Eenmaal per twee jaar worden de personeelsdossiers gecontroleerd op volledigheid.

5.5. Minimale gegevensverwerking

Een belangrijk beginsel voor het verwerken van persoonsgegevens is het principe dat deze gegevens toereikend zijn en beperkt tot wat noodzakelijk is voor het doeleinde. Voor het verlenen van gezondheidszorg worden de relevante gegevens opgenomen in het ECD. Hierbij wordt door de zorg- en hulpverleners steeds afgewogen of deze gegevens betrekking hebben op het zorg-, begeleidings, of behandelplan die met de bewoner of cliënt wordt vastgesteld. Wanneer gegevens geen betrekking hebben op dit plan, dan worden deze gegevens ook in principe niet vastgelegd.

5.6. Opslagbeperking

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doeleinde tenzij in de wetgeving een andere bewaartermijn is opgenomen. Orpea voert een archiefbeleid met het doel vast te stellen welke informatie wordt verzameld en gecreëerd, wat de bron van deze informatie is, wie en onder welke voorwaarden toegang heeft tot de informatie en onder welke voorwaarden de informatie wordt bewaard en vernietigd. Dit heeft grotendeels betrekking op persoonsgegevens maar daarnaast ook op de bedrijfsinformatie.

In 2021 is een onderzoek uit gevoerd met betrekking tot de bewaartermijnen. Uitkomsten zijn dat er verschillen zijn in de vastgestelde termijnen tussen de bedrijven, er verschillend wordt omgegaan met de toegang tot gegevens in rust, er geen bewust onderscheid wordt gemaakt in het gebruik van brongegevens en duplicaten en dat (digitale) gegevens na afloop van de bewaartermijn niet via een beheerst proces worden vernietigd. Op basis hiervan worden in 2022 maatregelen getroffen om ervoor te zorgen dat de opslag van gegevens in rust in overeenstemming met de beginselen van de AVG is.

5.7. Integriteit en vertrouwelijkheid

Voor het verlenen van de gezondheidszorg zijn gegevens nodig die betrekking hebben op de gezondheid van de cliënten. Vanwege het medisch beroepsgeheim hebben deze gegevens een vertrouwelijk karakter. Deze gegevens zijn opgeslagen in een ECD. Aan dit ECD zijn eisen gesteld ten aanzien van de integriteit en toegang van de opgeslagen gegevens. De leverancier is contractueel gebonden om maatregelen te treffen om de integriteit en vertrouwelijkheid te waarborgen.

Binnen de organisatie worden eisen gesteld aan de toegang tot gegevens in het ECD. Door middel van een autorisatiematrix zijn rechten in het ECD toegekend aan de zorgverleners zodat zij de beschikking hebben over de noodzakelijke gegevens om op een veilige en verantwoorde wijze de zorg te kunnen verlenen.

De toegang tot het ECD is beveiligd met tweefactor authenticatie. Hierbij is naast een combinatie van een gebruikersnaam en wachtwoord ook goedkeuring vanaf een mobiel apparaat (telefoon of tablet) noodzakelijk om toegang te krijgen tot het ECD.

De gebruikersactiviteiten in het ECD worden vastgelegd in logbestanden. Deze logbestanden worden minimaal vijf jaar bewaard en zijn toegankelijk voor de ICT-afdeling. Deze logbestanden worden gecontroleerd wanneer daar aanleiding voor is. Een systematische en periodieke controle van deze logbestanden is niet ingericht.

6. Beveiligingsmaatregelen

Orpea beschikt over een informatiebeveiligingsbeleid. Dit beleid is van toepassing op de gehele organisatie. Voor de implementatie en het onderhoud van de beveiligingsmaatregelen zijn afspraken gemaakt en contractueel vastgelegd met leveranciers van de applicaties waarin persoonsgegevens worden verwerkt, de verwerkersovereenkomsten. Dit beleidsdocument moet worden geactualiseerd waarbij de normen van NEN7510 als uitgangspunt worden genomen.

In 2021 is een start gemaakt met de monitoring door een gespecialiseerd bedrijf op het gebied van cybersecurity. Hierbij wordt de toegang tot het netwerk en de cloudapplicaties 24/7 bewaakt. Indien daartoe aanleiding is wordt ingegrepen om te voorkomen dat onbevoegden zich toegang verschaffen tot het netwerk en cloudapplicaties en daarmee tot persoonsgegevens. De specialisten van het bedrijf adviseren over het treffen van technische en organisatorische maatregelen.

De ISO maakt onderdeel uit van het ICT-team en heeft als taak de aanvullende beveiligingsmaatregelen te implementeren, te onderhouden en te reageren op incidenten. De implementatie van deze maatregelen wordt vastgelegd in beleid, processen en instructies. De ISO heeft ook als taak de bewustwording met betrekking tot informatieveiligheid binnen de organisatie te bevorderen. Hiervoor werkt de ISO nauw samen met de FG.

Hoewel de processen met betrekking tot de toegang tot het netwerk en applicaties volledig zijn ingericht en hierop actief wordt gemonitord is de procesdocumentatie is nog niet voor alle processen vastgelegd.

Wel is een proces ingericht voor het melden en afhandelen van datalekken. De beschrijving van het proces is beschikbaar in het handboek van de organisatie. Medewerkers kunnen een datalek melden via een knop op de homepage van het intranet of door een mail te sturen naar het contactpunt gegevensbescherming. De meldingen van datalekken worden direct in behandeling genomen en door de FG beoordeeld. Wanneer sprake is van een digitaal beveiligingsaspect dan wordt altijd de ISO ingeschakeld zodat snel maatregelen kunnen worden getroffen. De datalekken worden geregistreerd in een register van datalekken.

6.1. Organisatorische maatregelen

De werknemers zijn onderworpen aan een geheimhoudingsplicht. Dit betekent dat zij de informatie en gegevens die zij verwerken niet met anderen mogen delen tenzij dit noodzakelijk is voor de uitvoering van hun taken. Hierop zijn gedragsregels van toepassing. In deze gedragsregels is opgenomen dat het overtreden van deze geheimhoudingsplicht arbeidsrechtelijke consequenties kunnen hebben.

De toegang tot de persoonsgegevens is beperkt tot hetgeen de medewerkers nodig hebben voor hun werkzaamheden. Dat betekent dat de teams toegang hebben tot de persoonsgegevens van hun cliënten zodat de zorgverlening kan worden gepland, uitgevoerd en verantwoord. Om de zorgverlening te kunnen verantwoorden en declareren hebben medewerkers van administratieve afdelingen ook toegang tot cliëntgegevens, in bepaalde gevallen – wanneer dit noodzakelijk is – ook tot de gezondheidsgegevens.

Een belangrijk onderdeel van de organisatorische maatregelen is de bewustwording van de risico's die het verwerken van persoonsgegevens met zich meebrengen. Hiervoor worden regelmatig nieuwsberichten op het intranet geplaatst en wordt van actualiteiten en incidenten gebruik gemaakt om het bewustzijn van medewerkers te stimuleren.

In 2021 is gestart met het organiseren van themaweken waarbij een bepaald onderwerp in de schijnwerpers wordt gezet. Hiervoor worden een aantal artikelen gepubliceerd, is een poster te downloaden en kunnen medewerkers meedoen met een online quiz waarbij onder de deelnemers een cadeaubon wordt verloot. De volgende thema's zijn onder de aandacht gebracht: het herkennen en melden van datalekken, het maken en gebruiken van veilige wachtwoorden, de rechten van betrokkenen en het herkennen van phishing. Gedurende het jaar is het aantal deelnemers aan de themaweken gegroeid.

In september 2021 is een phishingtest uitgevoerd. Hierbij is een nep-phishing bericht naar alle medewerkers gestuurd waarbij wordt gemeten wie op de link in het bericht klikt. Uitkomst van de test is dat bijna 40% van degenen die de mail heeft ontvangen, ook op de 'onveilige' link heeft geklikt. Dat betekent dat aan de bewustwording op het gebied van phishing nog aandacht moet worden besteed.

Papieren gegevensdragers met daarop persoonsgegevens worden in gesloten ruimten opgeslagen zodat deze beschermd zijn tegen onbevoegde inzage, beschadiging en voortijdige vernietiging.

6.2. Technische maatregelen

De netwerkomgeving waarbinnen de persoonsgegevens worden verwerkt en toegang wordt verstrekt tot applicaties is strikt beveiligd. Hierbij zijn maatregelen getroffen om misbruik en aanvallen van buitenaf te weerstaan. De gegevens zijn binnen een cloud-omgeving opgeslagen en benaderbaar voor geautoriseerde gebruikers. De toegang wordt verstrekt op basis van de rechten die in het identity management systeem zijn vastgelegd.

De toegang tot het netwerk en de applicaties wordt zoals eerder aangegeven continu gemonitord. Hierdoor wordt snel ingegrepen wanneer er geprobeerd wordt om onrechtmatig toegang te verkrijgen tot het netwerk en de daarin opgeslagen gegevens. In 2021 is hiermee meerdere malen een poging tot onrechtmatige toegang voorkomen. Wanneer zich een incident – al dan niet een datalek – voordoet dan worden maatregelen getroffen om de beveiligingsinstellingen zodanig aan te passen dat de kans op herhaling wordt geminimaliseerd, dit is een continue verbetercyclus.

Met leveranciers van het netwerk, kernsysteem en applicaties waarbinnen persoonsgegevens worden verwerkt zijn afspraken gemaakt met betrekking tot het treffen van beveiligingsmaatregelen. Deze afspraken zijn vastgelegd in een verwerkersovereenkomst. Hierbij is overeengekomen dat de leverancier regelmatig de actuele beveiligingspatches installeert, back-ups maakt, PEN-testen uitvoert en versleutelde verbindingen gebruikt. De leverancier moet in staat zijn om aan te tonen dat de persoonsgegevens conform de afspraken worden verwerkt.

7. Gegevensbescherming bij ontwerp en door standaardinstellingen

7.1. Uitgangspunten in beleid

In het gegevensbeschermingsbeleid is opgenomen dat bij de ontwikkeling, implementatie en uitvoering van processen en systemen aantoonbaar rekening moet worden gehouden met gegevensbescherming. Hiervoor moeten nieuwe verwerkingen of wijzigingen in verwerkingen en systemen vooraf worden gemeld aan de FG.

Er is een werkinstructie beschikbaar waarin de uitvoering van een DPIA is beschreven. Hoewel deze uitgangspunten in het beleid zijn opgenomen en hiervoor een werkinstructie en werkdocumenten beschikbaar zijn is dit nog geen geborgd principe in de organisatie. In 2022 en daarna zal dit principe meer en meer in de organisatie en haar processen moeten worden ingebed.

7.2. Betrokkenheid FG bij nieuwe ontwikkelingen

Wanneer binnen Orpea zich ontwikkelingen voordoen die van invloed zijn op de bescherming van persoonsgegevens, dan wordt de FG in een vroeg stadium betrokken. De betrokkenheid bestaat uit het toezien op de naleving van de wettelijke verplichtingen en het verstrekken van advies op dit vlak. Als voorbeeld heeft Orpea in 2021 een nieuwe leverancier geselecteerd voor het werkplekbeheer. Hierbij zijn in de aanbesteding de verplichtingen die de wet stelt aan de verwerking van persoonsgegevens meegenomen en is de FG in het aanbestedingsproces betrokken geweest.

Dit geldt ook voor bijvoorbeeld samenwerkingen met gespecialiseerde ziekenhuizen, de samenwerking tussen Allerzorg, iCare en Coloriet voor het leveren van ongeplande nachtzorg in de regio Flevoland. Het laatste voorbeeld heeft geleid tot de uitvoering van een gezamenlijke DPIA om de risico voor betrokkenen te minimaliseren. Bij de totstandkoming van de DPIA en de voorgestelde maatregelen is de FG betrokken geweest.

PGZ heeft in 2021 vanwege de veranderingen in het declaratieproces het besluit genomen om van ECD te wisselen. Hierbij gaat PGZ over van Qurentis naar ONS (Nedap). Voordeel hierbij is dat hiermee het applicatielandschap verder wordt vereenvoudigd omdat andere bedrijven binnen de groep met hetzelfde ECD werken. Ook bij de selectie van deze leverancier is de FG betrokken geweest. Hierbij is gelet op de vereisten die de AVG stelt aan de verwerking van. De uitkomst hiervan is dat een DPIA is uitgevoerd op de implementatie en inrichting van het nieuwe ECD (zie verder hiervoor paragraaf 7.3 Uitgevoerde DPIA's).

7.3. Uitgevoerde DPIA's

Het uitvoeren van een DPIA is een complexe aangelegenheid. Hierbij is het verzamelen en beoordelen van de juiste informatie cruciaal voor het juist inschatten van de risico's en het formuleren van de maatregelen. Orpea heeft een DPIA-team opgericht zodat het uitvoeren van DPIA's gemakkelijker wordt gemaakt en kennis en ervaring op dit vlak wordt gebundeld. Het DPIA-team bestaat uit vier medewerkers die elk afkomstig zijn vanuit verschillende pijlers. De FG heeft het DPIA-team getraind en ondersteunt het team met advies. In een tweewekelijks overleg wordt de voortgang van de lopende DPIA's besproken en geeft de FG advies omtrent de uitvoering ervan.

In 2021 is gestart met een DPIA die zich heeft gericht op de implementatie en inrichting van het ECD van Nedap – Ons bij PGZ. De leden van het DPIA-team hebben bij de projectgroep informatie over de implementatie en inrichting verzameld. De juridische aspecten zijn door de FG beoordeeld. De oplevering van de DPIA vindt begin 2022 plaats.

8. Register van verwerkingsactiviteiten

Alle verwerkingen zijn opgenomen in een register van verwerkingsactiviteiten. In dit register is per werking de wettelijk vereiste informatie over de verwerking vastgelegd. Het register wordt onderhouden door de FG. Nieuwe verwerkingen en wijzigingen in bestaande verwerkingen worden bij de FG aangemeld.

De FG beoordeelt de aanmelding op de naleving van de wettelijke verplichtingen en onderzoekt indien nodig de verwerking wanneer daar aanleiding toe is. De nieuwe verwerkingen en wijzigingen in de bestaande verwerkingen worden opgenomen in het register van verwerkingsactiviteiten. Dit is een online register die – wanneer hier om wordt gevraagd – aan de toezichthouder ter inzage wordt gegeven.

Met het register wordt inzicht en overzicht gecreëerd van de verwerkingen van persoonsgegevens waarvoor Orpea verwerkingsverantwoordelijke is. Het register is onderdeel van de verantwoordingsplicht die op Orpea rust. Met het register kan Orpea aantonen dat de verwerkingen van persoonsgegevens aan de wettelijke vereisten voldoet.

9. Datalekken

9.1. Analyse

Inbreuken in verband met persoonsgegevens ofwel datalekken komen ondanks de getroffen maatregelen om persoonsgegevens te beveiligen, voor. In 2021 zijn 30 datalekken intern gemeld. Alle meldingen zijn door de FG in behandeling genomen.

Voor zestien datalekken konden risico's voor de rechten en vrijheden van betrokkenen niet worden uitgesloten. Deze datalekken zijn aan de Autoriteit Persoonsgegevens gemeld en zijn in alle gevallen ook de betrokkenen op de hoogte gebracht. In één geval is een melding ingetrokken omdat een verdwenen poststuk alsnog is teruggevonden. In geen van de gevallen is geconstateerd dat het datalek tot directe schade heeft geleid bij de betrokkenen.

Twee datalekken zijn buiten de wettelijke termijn van 72 uur na het ontdekken gemeld aan de toezichthouder. De oorzaak hiervan is dat de betrokken medewerkers het incident niet hadden herkend als een datalek waardoor deze intern te laat is gemeld. De vertraging van de melding is gemotiveerd aangegeven in de melding bij de toezichthouder.

In veertien gevallen bleek dat het datalek waarschijnlijk geen nadelig gevolg heeft gehad voor de betrokkenen. Deze datalekken zijn niet gemeld aan de Autoriteit Persoonsgegevens. Wel zijn deze opgenomen in het register van datalekken.

In de meeste gevallen blijkt dat het ontstaan van datalekken het gevolg is van menselijk handelen. Hierbij moet worden gedacht aan het verkeerd adresseren van poststukken en e-mails. Met dubbele controles en bewustwording zijn maatregelen getroffen om herhaling te voorkomen. Overige oorzaken zijn storingen in het ECD of systemen waarin persoonsgegevens worden verwerkt en waarbij deze tijdelijk niet toegankelijk zijn geweest.

9.2. Maatregelen

Alle incidenten die zijn gemeld hebben geleid tot verbeteringen van de beveiligingsmaatregelen. Dit betreft maatregelen op de instellingen voor de toegang tot het netwerk, organisatorische maatregelen zoals het verbeteren van processen en verduidelijken van instructies en het bewustmaken van medewerkers.

Een van de grootste gevaren voor de bescherming van persoonsgegevens is om via phishing toegang te krijgen tot de persoonsgegevens van cliënten en werknemers. Binnen de organisatie is uitgebreid aandacht is geweest voor het herkennen van deze berichten en op welke wijze gehandeld moet worden wanneer een medewerker een phishingmail ontvangt. Als onderdeel hiervan is een phishingtest uitgevoerd. Regelmatig wordt een nieuwsbericht op het intranet gezet en worden leidinggevenden gestimuleerd om dit onderwerp in het werkoverleg te bespreken.

10. Rechten betrokkenen

10.1. Privacyverklaring

De verwerking van persoonsgegevens brengt met zich mee dat de betrokkenen voorafgaand over de verwerking van de persoonsgegevens moet worden geïnformeerd. De bedrijven van Orpea hebben hiervoor een privacyverklaring op hun website gepubliceerd. Voor verschillende websites zijn deze verklaring aangepast zodat deze aan de informatieplicht van de AVG voldoet en de verwerking van persoonsgegevens transparant is voor de betrokkenen. De privacyverklaring wordt jaarlijks herzien of indien daartoe aanleiding is, eerder. Hiermee wordt beoogd dat de verklaring altijd overeenkomt met de verwerkingen van persoonsgegevens en de toepasselijke wet- en regelgeving hieromtrent.

10.2. Procedure uitoefening rechten

De betrokkene heeft ten aanzien van de verwerking van zijn persoonsgegevens een aantal rechten. Het gaat hier bijvoorbeeld om het recht van inzage, rectificatie, gegevenswissing en gegevensoverdracht. De betrokkene kan zijn rechten bij uitoefenen door per e-mail een verzoek in te dienen bij het contactpunt. Een rechtenverzoek wordt door de FG in ontvangst genomen en binnen de organisatie uitgezet. De FG ziet toe op een tijdige en juiste afhandeling van het verzoek.

De afdeling/team die de gegevens verwerkt, stelt de authenticiteit van het verzoek en de identiteit van de verzoeker vast. Eventueel wordt de verzoeker gevraagd zich te legitimeren. Het verzoek wordt beoordeeld waarbij de wet- en regelgeving in acht worden genomen. De FG ondersteunt de afdeling/team bij het beoordelen van het verzoek. Na de beoordeling wordt het verzoek uitgevoerd en de betrokkene hierover geïnformeerd. De betrokkene wordt in ieder geval binnen één maand na ontvangst van het verzoek over de afhandeling geïnformeerd. De beschreven procedure is in het handboek van de organisatie vastgelegd.

10.3. Ingediende verzoeken

In 2021 zijn zes verzoeken ingediend. In vijf gevallen betrof het een verzoek tot inzage van de gegevens en in één geval een verzoekt tot gegevenswissing. In alle gevallen is de verzoeker binnen een maand geïnformeerd over de afhandeling van het verzoek.

11. Realisatie ambities 2021

De realisatie van de ambities van 2021 heeft minder onder druk gestaan door COVID-19 dan in 2020, maar de effecten hiervan zijn wel merkbaar geweest. Ook hebben de overnames van de verschillende bedrijven in het eerste halfjaar tijd gevraagd van de organisatie waardoor de in 2020 gestelde ambities onder druk hebben gestaan.

11.1. Implementeren uitvoering DPIA's

Het voornemen om een DPIA-team op te richten en deze door de FG te trainen en te begeleiden is gerealiseerd. Het team bestaat uit vier medewerkers die verspreid binnen Orpea werkzaam zijn. In een tweewekelijkse online bijeenkomst worden de ontwikkelingen ten aanzien van de DPIA's met het team doorgesproken. Daarnaast wordt ingezet om het eigenaarschap van de DPIA's bij het management te beleggen zodat het draagvlak voor het treffen van maatregelen om de risico's voor de betrokkenen te minimaliseren, vergroot wordt. Het team is in 2021 gestart met twee DPIA's en hebben deze begin 2022 afgerond.

11.2. Bewustwording medewerkers

In paragraaf 6.1 zijn de themaweken al genoemd. Met het organiseren van deze themaweken is een format ontstaan waarop de bewustwording in de komende jaren verder kan worden gestimuleerd. Voor 2022 zijn vier nieuwe themaweken gepland.

11.3. Overzicht verbonden partijen

Binnen de zorgsector wordt tussen zorgaanbieders intensief samengewerkt om het zorgaanbod af te stemmen op de zorgvraag vanuit de markt. Daarnaast zijn tal van leveranciers betrokken bij de primaire en ondersteunende processen waarbij persoonsgegevens worden verwerkt. Hierdoor is het wenselijk én noodzakelijk om zicht te krijgen op welke partijen betrokken zijn bij de verwerking van persoonsgegevens.

De samenwerking en levering van diensten zijn in de meeste gevallen vastgelegd in overeenkomsten, waarbij in bepaalde gevallen ook verwerkersovereenkomsten zijn gesloten. In deze overeenkomsten zijn de wederzijdse rechten en plichten vastgelegd die onder andere betrekking hebben op de verwerking van persoonsgegevens. In 2021 is gestart met het in kaart brengen van deze overeenkomsten.

12. Ambities 2022

De onderstaande ambities zijn als beleidsdoelstellingen voor 2022 opgenomen in het gegevensbeschermingsbeleid. Hierover wordt in de verantwoordingsverklaring van 2022 verantwoording afgelegd.

12.1. Privacy-by-design

Bij het ontwerp van nieuwe en gewijzigde producten, processen en systemen wordt aantoonbaar rekening gehouden met gegevensbescherming. Dit betekent dat in 2022 meer DPIA's worden uitgevoerd om de risico's voor betrokkenen te minimaliseren waar het gaat om nieuwe ontwikkelingen. Hierbij moet worden gedacht aan de implementatie van nieuwe software en het ontwikkelen van nieuwe dienstverlening, maar ook aan de beoordeling van bestaande verwerkingen.

Het DPIA-team speelt bij de uitvoering van de DPIA's een belangrijke rol. Daarom wordt dit team intensief door de FG begeleid en regelmatig getraind. Daarnaast vormt de FG een belangrijk schakelpunt tussen de verwerkingsverantwoordelijken en het team waar het gaat om toezicht en advies met betrekking tot de naleving van wet- en regelgeving.

12.2. Bewaartermijnen

In het zorgverleningsproces worden veel persoonsgegevens vastgelegd. Dit geldt ook voor de ondersteunende processen zoals de personeels- en financiële administratie. Wanneer persoonsgegevens niet meer nodig zijn, moeten deze worden vernietigd tenzij een wettelijke bewaartermijn van toepassing is. Een bekend voorbeeld is dat na het afsluiten van het medisch dossier, de gegevens gedurende 20 jaar bewaard moeten worden. In wet zijn verschillende termijnen benoemd.

Om te waarborgen dat persoonsgegevens gedurende de wettelijke termijnen worden bewaard en na afloop daarvan worden vernietigd wordt een proces ingericht om deze termijnen te bewaken. Tevens wordt een proces ingericht voor de besluitvorming en vernietiging van persoonsgegevens. Hiermee kan worden aangetoond dat aan de wettelijke verplichtingen wordt voldaan.

12.3. Samenwerking

Het zorgaanbod van de verschillende bedrijven van Orpea is op bepaalde vlakken complementair. Bijvoorbeeld: een cliënt van Orpea ontvangt zorg thuis totdat dit niet meer gaat. Dit kan tot gevolg hebben dat de cliënt een bewoner van een woonhuis van Orpea wordt. Een ander voorbeeld is dat een bewoner van een woonhuis gespecialiseerde wondzorg nodig heeft. Omdat dit nu nog verschillende verwerkingsverantwoordelijken betreft is het belangrijk dat de zorgbedrijven onderling afspraken maken over de uitwisseling van persoonsgegevens zodat enerzijds een sluitend zorgaanbod is en anderzijds aan de wetgeving wordt voldaan.