Verantwoordingsverklaring inzake gegevensbescherming 2022

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

Mei 2023

Inhoudsopgave

1. Inleiding

1.1. Doel verklaring

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

Zonder deze gegevens kan geen zorg geleverd worden en kan de organisatie niet functioneren. De betrokkenen verstrekken ons hun gegevens in het vertrouwen dat wij daar op een integere, juiste en vertrouwelijk wijze mee omgaan.

Met deze verklaring leggen de bedrijven van Orpea in Nederland[1] (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 beveiligingsmaatregelen worden aangetoond.

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 proces- en systeemeigenaren 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 ICT-manager, de FG en de information security officer (ISO).

De FG verzamelt informatie met betrekking tot de effectieve werking van de beveiligingsmaatregelen om aan te tonen in hoeverre Orpea aan de wettelijke verplichtingen voldoet. Hiervoor worden verschillende registers bijgehouden. De FG rapporteert hierover periodiek aan de Raad van Bestuur en brengt advies uit over de naleving van wettelijke verplichtingen.

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 naleving van de wettelijke verplichtingen met betrekking tot de verwerking van persoonsgegevens in 2022. De FG licht in de 'Mededeling functionaris voor gegevensbescherming' toe welke rol deze heeft gehad met betrekking tot zijn wettelijke taken. De verantwoording wordt onderbouwd door de overige hoofdstukken van de verklaring.

[1] Zie hoofdstuk 4 Organisatiebeschrijving

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.
ETDR	Elektronische toedienregistratie, een applicatie waarin de toediening van medicatie wordt vastgelegd en verantwoord.
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

Deze verklaring heeft betrekking op de ondernemingen van Orpea in Nederland met uitzondering van Dagelijks Leven BV. Met deze verklaring legt de Raad van Bestuur verantwoording af aan het maatschappelijk verkeer over de naleving van de wettelijke verplichtingen die op de verwerking van de persoonsgegevens rusten.

Om de gezondheidszorg te kunnen verlenen verwerkt Orpea op grote schaal persoonsgegevens van bewoners, cliënten en (zorg)professionals, waaronder gegevens over de gezondheid van bewoners en cliënten. Het verbod op de verwerking van deze gezondheidsgegevens is niet van toepassing omdat deze gegevens alleen voor het verstrekken van gezondheidszorg worden verwerkt. De naleving van wettelijke verplichtingen zijn opgenomen in het gegevensbeschermingsbeleid van de organisatie. In hoofdstuk 11 wordt toegelicht in welke mate de beleidsdoelstellingen van 2022 zijn gerealiseerd en in hoofdstuk 12 zijn de doelstellingen van 2023 opgenomen. Het beleid is voor elke (zorg)professional beschikbaar.

Belangrijk onderdeel van het beleid is het voeren van een register van verwerkingsactiviteiten. In dit register zijn alle reguliere verwerkingen zijn opgenomen. Aanvullingen en wijzigingen worden door de FG beoordeeld en in het register bijgehouden. Om deze gegevens te beschermen tegen onrechtmatige verstrekking, diefstal, verminking of verlies zijn organisatorische en technische maatregelen getroffen. Over de toepassing en effectiviteit van deze maatregelen wordt elk kwartaal verslag uitgebracht en – indien daartoe aanleiding is – worden aanvullende maatregelen getroffen. In hoofdstuk 6 worden deze maatregelen verder toegelicht.

Ondanks dat er maatregelen zijn getroffen kan het mis gaan en ontstaan datalekken. Meest in het oog springende datalek in 2022 betrof CarenZorgt, de persoonlijke gezondheidsomgeving (PGO) van Nedap waarbij een hacker via het PGO toegang heeft gehad tot het ECD van een aantal bewoners van Orpea. Gelukkig heeft dit datalek niet tot directe schade aan betrokkenen geleid. In hoofdstuk 9 worden de oorzaak en gevolgen van de overige datalekken verder toegelicht.

Elke betrokkene kan de rechten ten aanzien van de verwerking van diens persoonsgegevens uitoefenen. De organisatie faciliteert deze rechten door elk verzoek binnen de wettelijke termijn te beantwoorden. In hoofdstuk 10 is toegelicht hoe daarmee is omgegaan.

Bij de start van nieuwe verwerkingen of wijzigingen in bestaande verwerkingen moet worden beoordeeld of dit hoge risico's voor de rechten en vrijheden voor de betrokkenen tot gevolg heeft. In sommige gevallen moet een DPIA worden uitgevoerd. Orpea heeft hiervoor een team samengesteld die de organisatie ondersteunt bij de uitvoering hiervan. Het team wordt jaarlijks door de FG bijgeschoold en is in 2022 uitgebreid tot zes leden. In 2022 zijn een aantal DPIA's afgerond, dit wordt in hoofdstuk 7 toegelicht.

Voor 2023 is de ambitie om de bescherming van de persoonsgegevens verder te optimaliseren door de effectiviteit van maatregelen naar aanleiding van datalekken, signalen en onderzoeken vast te volgen en vast te stellen. Wij vinden het belangrijk om verbeteringen in de organisatie en processen te verankeren zodat de naleving van de wettelijke verplichtingen die op de verwerkingen rusten kunnen worden aangetoond.

Anton van Mansum,

Bestuurder

Laurent Guillot,

Bestuurder

3. Mededeling functionaris gegevensbescherming

3.1. Aanwijzing

Orpea verwerkt op grote schaal gezondheidsgegevens en daarmee is sprake van een grootschalige verwerking van bijzondere categorieën van gegevens. Orpea heeft mij als FG aangesteld, waarmee aan de wettelijke verplichting wordt voldaan.[2] Als FG voer ik mijn taken op concernniveau uit en ben ik gemakkelijk vanuit elke locatie te bereiken. Om mijn taken goed te kunnen uitvoeren heb ik de Leergang functionaris gegevensbescherming in 2019 afgerond.[3] Daarnaast volg ik diverse inhoudelijke cursussen en woon ik regelmatig relevante (netwerk)bijeenkomsten en congressen bij. Mijn taken vervul ik onafhankelijk, onpartijdig en integer.

3.2. Positie

Het is belangrijk dat ik tijdig wordt betrokken bij aangelegenheden die van invloed (kunnen) zijn op de bescherming van persoonsgegevens en dat ik ondersteund wordt in de uitoefening van mijn taken. Vanwege de dynamiek van de organisatie en de ontwikkelingen hierbij horen, is de betrokkenheid niet altijd tijdig. Wel word ik voldoende door de organisatie ondersteund om mijn taken naar behoren uit te voeren. Om de betrokkenheid aandacht te geven is er regelmatig overleg met de directeuren van de pijlers.[4] Dit vereist continue aandacht. Naast mijn taken ben ik betrokken geweest bij de afhandeling van klachten en van schades en verzekeringen. In 2023 worden deze neventaken overgedragen.

Elk kwartaal rapporteer ik over de naleving van de wettelijke verplichtingen aan de Raad van Bestuurd. Deze kwartaalrapportages worden in het overleg met de Raad van Bestuur gesproken. De door mij verstrekte adviezen zijn door de organisatie opgevolgd.

3.3. Taken

Als FG zie ik toe op naleving van de wettelijke verplichtingen die op de verwerking van de persoonsgegevens rusten. Hiervoor verzamel ik informatie door locatiebezoeken en gesprekken met (zorg)professionals. Daarnaast zie ik toe op een correcte afhandeling van datalekken en rechtenverzoeken. Ik adviseer de organisatie over de naleving van de verplichtingen en geef daarbij aan binnen welke kaders de mogelijkheden liggen. Tot slot stimuleer ik de bewustwording van de (zorg)professionals door het organiseren van themaweken, het schrijven van artikelen en het geven van presentaties en trainingen.

Frans Schreuder

Functionaris Gegevensbescherming

[2] Art. 37 AVG
[3] Via Duthler Academy
[4] Zie paragraaf 4.2 Pijlerstructuur

4. Organisatiebeschrijving

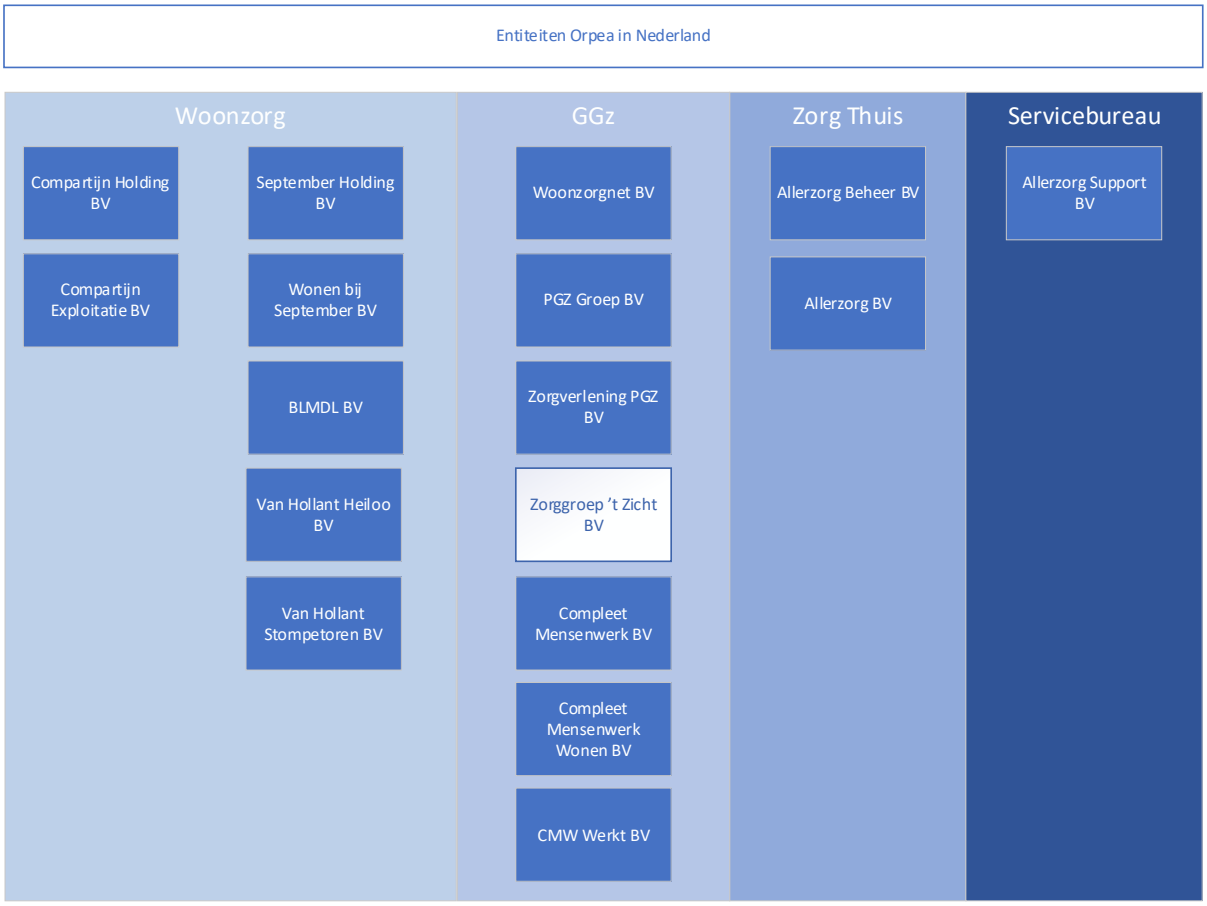
4.1. Algemeen

Orpea Group 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 Zorg Thuis. Elke pijler wordt aangestuurd door een eigen management team. De organisatie wordt ondersteund door een servicebureau. Hier worden de bulkprocessen uitgevoerd zoals de personeels- en salarisadministratie, financiële administratie, kwaliteitsmanagement en ICT.

In figuur 1 is in een overzicht de structuur van de betrokken entiteiten opgenomen.



Figuur 1

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, Van Hollant Heiloo BV en Van Hollant Stompetoren BV)
- Woonzorgnet BV (inclusief Zorggroep ’t Zicht BV, Compleet Mensenwerk BV, Compleet Mensenwerk Wonen BV en CMW Werkt BV)

Zorggroep ’t Zicht BV is per 28 december 2022 gefuseerd met Woonzorgnet BV.

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 bewoners binnen woonlocaties en bij cliënten thuis in de vorm van verpleging en verzorging, begeleiding en behandeling. Alle overige verwerkingen van persoonsgegevens, zoals die van (zorg)professionals zijn gerelateerd aan en afgeleid van deze doeleinden. 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 de verwerking van gezondheidsgegevens valt daarmee onder deze uitzondering.

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 bewoner/cliënt 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 bewoners en cliënten is het van groot belang dat de gegevens 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 persoonsniveau 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. In 2022 hebben PGZ en Woonzorgnet de overstap gemaakt naar het ECD ONS van Nedap. Hiermee is een begin gemaakt voor het vereenvoudigen van het applicatielandschap binnen Orpea. Allerzorg zal begin 2023 ook gebruik gaan maken van ONS.

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 ook 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 niet vastgelegd.

5.6. Opslagbeperking

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doeleinde tenzij in de wetgeving een 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 wanneer deze vernietigd moeten worden. 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 is in 2022 een start gemaakt met het nemen van maatregelen om ervoor te zorgen dat de opslag van gegevens in rust in overeenstemming met de beginselen van de AVG is. Deze maatregelen worden in 2023 verder uitgewerkt en geïmplementeerd.

5.7. Integriteit en vertrouwelijkheid

Voor het verlenen van de gezondheidszorg zijn gegevens nodig die betrekking hebben op de gezondheid van de bewoners en cliënten. 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 nog 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.

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.

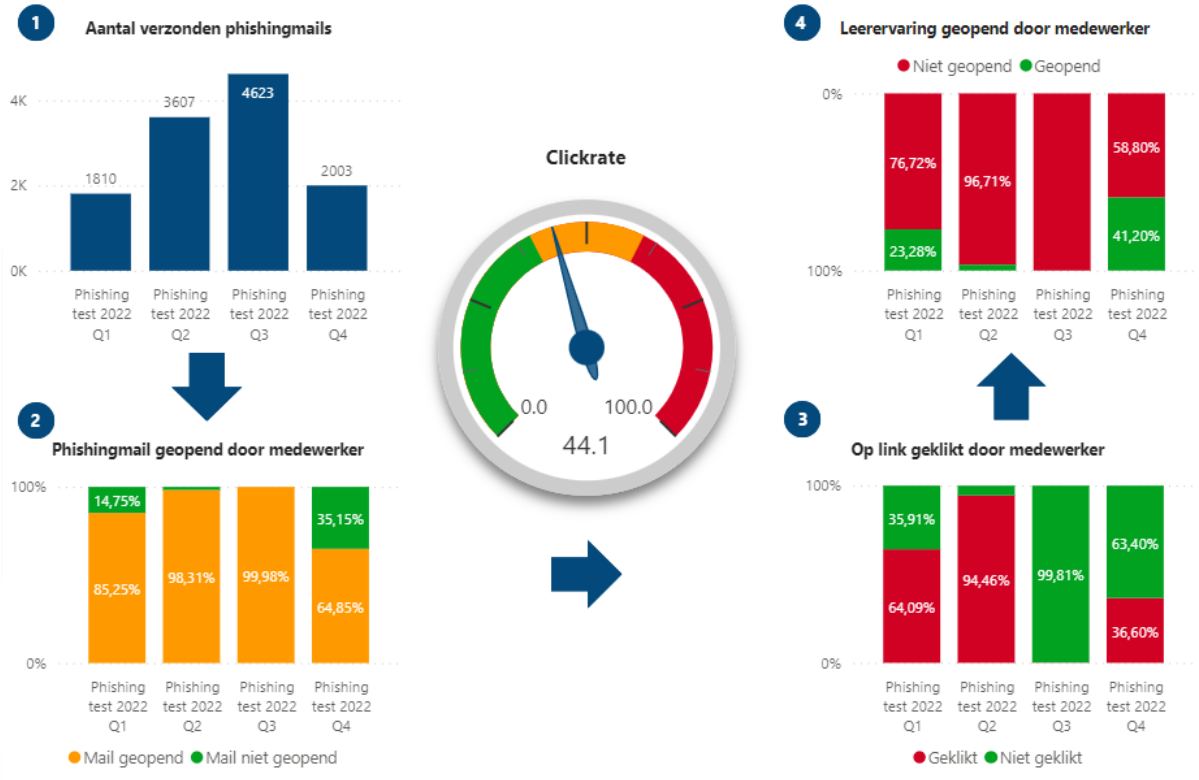
De toegang tot de persoonsgegevens is beperkt tot hetgeen de medewerkers nodig hebben voor hun werkzaamheden. Dat betekent dat de teams toegang hebben tot de persoonsgegevens van hun bewoners en cliënten zodat de zorgverlening kan worden gepland, uitgevoerd en verantwoord. Om de zorgverlening te kunnen 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 het bevorderen van 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. In 2022 is hiermee doorgegaan. Tijdens een themaweek 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: 'bewaartermijnen', 'toestemming', 'toegang dossier' en 'delen

persoonsgegevens'. Hoewel gedurende het jaar het aantal deelnemers aan de themaweken is gegroeid wordt nog niet iedereen bereikt. De afdeling Communicatie is betrokken om de timing van de themaweken met andere activiteiten af te stemmen en om de kanalen te gebruiken zodat zoveel mogelijk mensen worden bereikt. In 2023 zullen daarvan de resultaten zichtbaar moeten worden.

In 2022 is in elk kwartaal een phishingtest uitgevoerd. Hierbij is een nep-phishing bericht naar alle medewerkers gestuurd waarbij wordt gemeten welk percentage ontvangers op de link in het bericht heeft geklikt.



Figuur 2

De gemiddelde clickrate (het percentage gebruikers dat de phishingmail heeft ontvangen en op de link heeft geklikt) is gemiddeld 44,1%[5]. Hierbij moet worden aangetekend dat de test van het derde kwartaal onbedoeld door het SPAM-filter is tegengehouden. De gemiddelde clickrate ligt iets boven de doelstelling van maximaal 40%.

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-managementsysteem 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 2022 is hiermee meerdere malen

[5] Figuur 2

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 in overeenstemming met de afspraken en wet- en regelgeving worden verwerkt.

In overleg met het hoofdkantoor in Frankrijk hebben is besloten om over te stappen naar een centraal beheerd endpoint beveiliging. Deze beslissing is genomen met als doel om meer zichtbaarheid op dreigingen te krijgen en om vroegtijdig in te kunnen grijpen. Met de uitrol van dit product hebben we deze doelstelling kunnen behalen en zijn we nu beter in staat om onze systemen te beschermen tegen cyberaanvallen.

Daarnaast hebben we in het afgelopen jaar een kernteam informatiebeveiliging opgesteld binnen de IT-afdeling. Dit team bestaat uit verschillende disciplines vanuit de techniek, en zorgt voor een integrale aanpak van onze informatiebeveiliging. Dit heeft geleid tot een verbeterde samenwerking en heeft daarnaast gezorgd voor een verhoogd bewustzijn van de beveiligingsrisico's binnen onze organisatie.

In 2022 hebben we besloten om de uitgifte van werkplekken in-house uit te voeren. Door deze verandering hebben we meer controle gekregen op de inrichting van de werkplekken en de kwaliteit van uitgifte. Dit heeft niet alleen geleid tot betere efficiëntie en meer tevredenheid bij onze medewerkers, maar heeft ons meer controle gegeven over de beveiliging van de informatie.

Helaas heeft zich in het afgelopen jaar ook een informatiebeveiligingsincident voorgedaan bij een van onze leveranciers, wat impact heeft gehad op onze cliënten. Dankzij ons incidentmanagementproces hebben we adequaat kunnen handelen en zijn we transparant geweest richting onze cliënten. Dit heeft ook bijgedragen aan de bevestiging van het vertrouwen dat onze cliënten in ons stellen.

Wij hechten veel waarde aan onze informatiebeveiliging en streven ernaar om deze continu te verbeteren. Wij zullen dan ook blijven investeren in de beveiliging van onze systemen en processen, om zo de veiligheid van onze gegevens en die van onze cliënten te waarborgen.

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. Hoewel deze uitgangspunten zijn opgenomen in het beleid moet Orpea nog een stap maken om deze uitgangspunten daadwerkelijk te realiseren.

7.2. Betrokkenheid FG bij ontwikkelingen

Om toe te zien op naleving van wettelijke bepalingen binnen het kader van de verwerking van persoonsgegevens is het noodzakelijk dat de FG tijdig wordt geïnformeerd over ontwikkelingen op dit vlak.

In 2022 heeft de FG toegang gehad tot de notulen van het centraal management team, maar heeft geen gesprekken gevoerd met de Raad van Bestuur met betrekking tot de kwartaalrapportages die de FG naar het bestuur heeft gestuurd. Via de bestuurssecretaris is de FG over de ontwikkelingen geïnformeerd.

Bij het betrekken van derden voor de verwerking van persoonsgegevens is het noodzakelijk dat vooraf wordt vastgesteld binnen welke kaders persoonsgegevens vanuit de organisatie door betrokkenen kunnen worden verwerkt. Hierbij moeten de rollen van de betrokken partijen worden bepaald met de daarbij behorende waarborgen om de persoonsgegevens tegen onrechtmatige verwerking te beschermen.

Het aangaan van overeenkomsten met derde partijen[6] binnen Orpea is onvoldoende gereguleerd en verloopt niet altijd volgens een beheerst proces. Het gevolg is dat de FG niet in alle gevallen tijdig een advies over de naleving van de wettelijke bepalingen heeft kunnen verstrekken, bijvoorbeeld over de rollen van partijen binnen de verwerking, het vastleggen van afspraken in een verwerkersovereenkomst of een regeling gezamenlijke verwerkingsverantwoordelijkheid, de te nemen beveiligingsmaatregelen of het uitvoeren van een DPIA.

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 treffen van maatregelen om de rechten en vrijheden van betrokkenen te beschermen. Orpea heeft de beschikking over een DPIA-team zodat de kennis en ervaring op dit vlak wordt gebundeld. Het DPIA-team bestaat uit zes 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.

Er zijn vier DPIA's gestart en er zijn drie DPIA's afgerond. De DPIA's hebben betrekking op de verwerking van persoonsgegevens van bewoners en cliënten in zorginformatiesystemen waarbij nieuwe software in gebruik genomen is. Het gaat om de overgang van de ECD's van PGZ, Woonzorgnet en Allerzorg[7] naar ONS (van leverancier Nedap) en om de installatie van een nieuwe versie van een ETDR bij Wonen bij September.

[6] Uitgezonderd (woon)zorg-, arbeids-, zorgfinancierings- en huurovereenkomsten
[7] Deze DPIA is niet afgerond.

Maatregelen van eerder uitgevoerde DPIA zijn niet gevolgd. Daarom is per september 2022 een register van maatregelen opgezet waarmee de opvolging en effectiviteit van geformuleerde maatregelen door de FG wordt gemonitord. Over het register wordt eenmaal per kwartaal aan de Raad van Bestuur gerapporteerd. Het register houdt ook maatregelen bij die naar aanleiding van datalekken, signalen, klachten en onderzoeken worden genomen.

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 2022 zijn 39 datalekken intern gemeld (30% meer dan in 2021). Alle meldingen zijn door de FG in behandeling genomen. Vermoedelijke oorzaak van de stijging van het aantal datalekken is de toegenomen bewustwording om datalekken intern te melden.

Van zeventien 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 geen van de gevallen is geconstateerd dat het datalek tot directe schade heeft geleid bij de betrokkenen.

Vijf 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 in eerste instantie 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. Alle datalekken zijn opgenomen in het register van datalekken. Dit register wordt beheerd door de FG.

9.2. Maatregelen

Naar aanleiding van de datalekken zijn maatregelen getroffen om herhaling te voorkomen. De toepassing en effectiviteit van deze maatregelen wordt door de FG bewaakt en hierover wordt eenmaal per kwartaal over gerapporteerd aan de Raad van Bestuur.

De maatregelen hebben betrekking op organisatorische en technische aspecten of een combinatie daarvan. Voorbeelden zijn het aanpassen van instellingen in software, het wijzigen van werkinstructies, het geven van presentaties om de bewustwording te vergroten en het maken van aanvullende afspraken met leveranciers.

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 is 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.

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 diens rechten 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 aan de hand van opgevraagde informatie (bijvoorbeeld met de laatste drie cijfers van het BSN in combinatie met de geboortemaand en -jaar). 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 2022 zijn twaalf verzoeken ingediend. Tien verzoeken hadden betrekking op het recht van inzage van de gegevens. Twee verzoeken hadden betrekking op gegevenswissing. Voor tien verzoeken geldt dat de verzoeker binnen de wettelijke termijn van één maand inhoudelijk is geïnformeerd over de afhandeling van diens verzoek. De overige twee verzoekers zijn buiten deze termijn inhoudelijk over hun verzoek geïnformeerd.

11. Realisatie ambities 2022

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. Privacy-by-design

De concrete doelstelling om drie DPIA's in 2022 te hebben afgerond is behaald. Het DPIA-team is door het hele jaar actief geweest met het uitvoeren van de DPIA's. Het team wordt voortdurend ondersteund door FG. De opdrachten voor het uitvoeren van DPIA's worden vanuit de organisatie aan het team verstrekt. Het team koppelt de risico's en maatregelen terug aan de opdrachtgever die eigenaar is van de te treffen maatregelen.

11.2. Bewaartermijnen

Naar aanleiding van het onderzoek dat eind 2021 is uitgevoerd naar de bewaartermijnen binnen de organisatie is ingezet om de persoonsgegevens na afloop van de bewaartermijn volgens een beheerst proces te vernietigen. Het ontwerp van dit proces is in gang gezet door de afdeling Kwaliteit en Veiligheid in samenwerking met ICT en wordt naar verwachting in 2023 verder in de organisatie geïmplementeerd. Het proces verdient nog zeker de aandacht om te waarborgen dat de doelstelling in 2023 in z'n geheel wordt gehaald.

11.3. Samenwerking

De organisatie kent verschillende entiteiten die in drie verschillende pijlers zijn georganiseerd. Deze entiteiten werken steeds meer met elkaar samen en maken gebruik van elkaars systemen, medewerkers en ook gegevens. Binnen deze samenwerking worden persoonsgegevens tussen de verschillende hulpverleners uitgewisseld. De bewoner/cliënt krijgt hiermee de ondersteuning die nodig is zonder dat er een andere organisatie wordt ingezet. Een risico hierbij is er meer persoonsgegevens worden gedeeld dan noodzakelijk is en waarvoor een wettelijke basis is. Om dit risico te beheersen is voorgesteld om een convenant te sluiten tussen de pijlers waarin afspraken zijn gemaakt over hoe met de onderlinge uitwisseling van persoonsgegevens wordt omgegaan. Vanwege de aankomende bestuurswissel wordt het convenant begin 2023 aan het management voorgelegd.

12. Ambities 2023

De onderstaande ambities zijn als beleidsdoelstellingen voor 2023 opgenomen in het gegevensbeschermingsbeleid. Hierover wordt in de verantwoordingsverklaring van 2023 verantwoording afgelegd.

12.1. Bewaken maatregelen

Datalekken, DPIA's en onderzoeken hebben één ding gemeen: er vloeien maatregelen uit voort die de bescherming van persoonsgegevens moet verbeteren. Door het treffen van de maatregelen worden de risico's voor de betrokkenen en organisatie steeds verder verkleind. Na het afhandelen van een datalek, het opleveren van een DPIA of onderzoek neemt het verantwoordelijke management de voorgestelde/aanbevolen maatregelen. De FG bewaakt dat de maatregelen worden getroffen en worden geëvalueerd op toepassing en effectiviteit.

12.2. Bewustwording

Medewerkers zijn de belangrijkste schakel voor de bescherming van persoonsgegevens. Om die reden is een van de wettelijke taken van de FG het stimuleren van het bewustzijn van degenen die met persoonsgegevens werken. Hiervoor worden activiteiten georganiseerd en trainingen in de Academie geplaatst. Dit betreft twaalf trainingen waarvan er drie voor de medewerkers verplicht worden gesteld.

12.3. Rechten betrokkenen

Regelmatig worden verzoeken tot inzage in het dossier of het vernietigen van gegevens ingediend. Na ontvangst wordt beoordeeld of het verzoek kan worden gehonoreerd en wordt de betrokkene daarover geïnformeerd. Wettelijk gezien zijn er termijnen gesteld aan de afhandeling van een dergelijk verzoek. Daarnaast moet de indiener van het verzoek juist worden geïnformeerd. De functionaris gegevensbescherming bewaakt de termijn van afhandeling en beoordeelt of de verzoeker juist is geïnformeerd.