ALLERZORG

Verantwoordingsverklaring inzake gegevensbescherming 2020

Verantwoording van Allerzorg aan betrokkenen over het voldoen aan wet- en regelgeving op het gebied van bescherming van persoonsgegevens

ALLERZORG

Inhoudsopgave

1. Inleiding

1.1. Doel verklaring

Als specialist in zorg thuis verlenen onze zorgverleners dagelijks verpleging, verzorging en begeleiding aan cliënten in heel Nederland. Hiervoor is het noodzakelijk dat onze zorgverleners op de hoogte zijn van de gezondheidstoestand van de cliënten en weten waarmee zij in het kader van de zorgverlening rekening moeten houden. Daarnaast hebben we ook gegevens van onze 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 Allerzorg geen zorg leveren. De betrokkenen verstrekken ons hun gegevens in het vertrouwen dat deze op een integere, juiste en vertrouwelijk wijze worden verwerkt.

Met deze verklaring legt Allerzorg 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 Allerzorg 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 worden 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), FG (adviseert o.g.v. wetgeving en de praktijk), ISO[1] (adviseert op technisch vlak).

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 2020. De FG licht in de ‘Mededeling functionaris voor gegevensbescherming’ toe welke rol hij heeft gehad met betrekking tot zijn wettelijke taken.

[1] Information Security Officer

2. Mededeling Raad van Bestuur

Het jaar 2020 is een bijzonder jaar geworden voor iedereen, ook voor Allerzorg. De invloed van COVID-19 op de dagelijkse gang van zaken is duidelijk merkbaar geweest. Dit heeft tot nieuwe uitdagingen en vraagstukken geleid. Toen in maart 2020 de eerste lockdown werd afgekondigd en de omvang van de crisis waar Nederland zich in bevond duidelijk begon te worden is direct een coronateam ingericht met als taak de Raad van Bestuur en de rest van de organisatie te adviseren met betrekking tot de maatregelen om gevolgen van COVID-19 zo beperkt mogelijk te houden.

Want ondanks de pandemie hebben onze cliënten dagelijks zorg nodig en draaiden de processen en systemen gewoon door. De vraagstukken hadden niet alleen betrekking de infectiepreventie maar ook op gegevensbescherming. Vragen als hoe met het testen van medewerkers om te gaan, het opvragen en vastleggen van testuitslagen en weten wie is gevaccineerd zijn relevant geworden. Hierbij moeten enerzijds rekening houden met de veiligheid en welzijn van de cliënten, anderzijds moeten de persoonlijke levenssfeer van de betrokkenen respecteren. Samen met de FG is hierin een verantwoord evenwicht gevonden.

De lockdown had ook tot gevolg dat thuiswerken de norm werd, vergaderingen vrijwel helemaal online plaatsvonden en zorg op afstand werd geleverd. Dat stelde eisen aan de stabiliteit en veiligheid van het online werken. Hierbij is gebleken dat Allerzorg beschikt over een flexibele infrastructuur die de omslag in het werken prima heeft doorstaan. Wel zijn er incidenten geweest waarbij persoonsgegevens betrokken waren. De datalekken waarbij sprake was van een risico voor betrokkenen hebben we gemeld bij de Autoriteit Persoonsgegevens en we hebben ook de betrokkenen hierover geïnformeerd. Deze incidenten hebben geleid tot maatregelen om de infrastructuur en applicaties nog beter te beveiligen.

Andere ontwikkelingen gingen in 2020 gewoon door. In maart 2020 werd Compartijn onderdeel van Orpea waarbij de woonzorgtak van de organisatie verdubbelde. De stafafdelingen van Allerzorg hebben de overname van de ondersteunende processen gerealiseerd. Met deze ontwikkeling wordt verder gebruik gemaakt van de voordelen van schaalgrootte. Tegelijkertijd stelt dit hoge eisen aan de digitale infrastructuur en de beveiliging ervan. Dit zal in de komende jaren een belangrijke uitdaging blijven.

Een andere uitdaging is het inbedden van privacy-by-design. Het principe dat bij de ontwikkeling van processen en systemen de bescherming van persoonsgegevens een basisvoorwaarde is. Dit is een van de beleidsdoelstellingen voor 2021. We zorgen er hiermee voor dat het respectvol omgaan met persoonsgegevens en het voldoen aan de wettelijke eisen de norm is.

Roy Rempe,

Bestuurder

Loïc Batesti

Bestuurder

Mei 2021

3. Mededeling functionaris gegevensbescherming

3.1. COVID-19

Iedereen heeft in 2020 te maken gehad met de effecten van COVID-19, zo ook Allerzorg. De crisis die COVID-19 veroorzaakte heeft ervoor gezorgd dat bepaalde en geplande ontwikkelingen zijn vertraagt of zelf niet door zijn gegaan. Voor andere onderwerpen heeft het juist voor een versnelling gezorgd. Een voorbeeld is het op grote schaal vanuit huis werken waarbij fysieke ontmoetingen plotseling werden omgezet in digitale vergaderingen. Alle contacten moesten op afstand tot stand komen en dat leidde tot vraagstukken over hoe veilig vanuit huis te werken en te communiceren.

Ook leidde COVID-19 tot hele andere vraagstukken, zoals wie wordt getest en besmet is met het virus en wie gevaccineerd is en wie (nog) niet. En dat alles binnen het kader van de dan geldende wet- en regelgeving, die niet helemaal toegerust is op deze extreme omstandigheden. Als FG heb ik een bijdrage kunnen leveren aan het verschaffen van duidelijkheid over wettelijke bepalingen die hierop van toepassing zijn.

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 competenties 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.

Vanwege COVID-19 is het niet mogelijk gebleken om in 2020 het PE-programma van de opleiding te volgen. Om tóch 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. Voor 2021 wordt ervan uitgegaan dat een PE-programma weer kan worden opgepakt. 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 raak steeds meer ingebed in de organisatie en blijft zich ontwikkelen zoals ook de organisatie blijft ontwikkelen. In 2020 en voorgaande jaren heb ik ingezet om de organisatie zoveel mogelijk te informeren en te adviseren over de naleving van de AVG en aanpalende wet- en regelgeving.

Dit zal ik ook in 2021 blijven doen maar 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

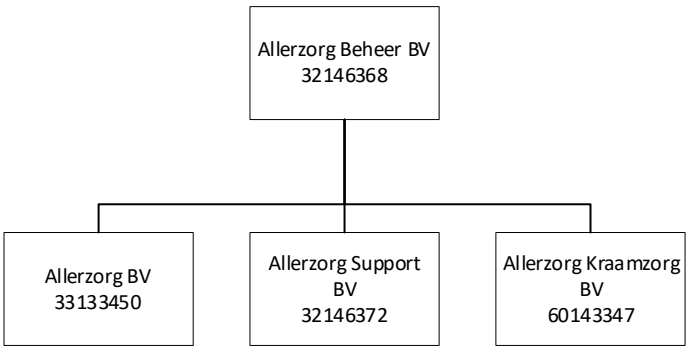
Mei 2021

4. Organisatiebeschrijving

4.1. Algemeen

Allerzorg is onderdeel van Orpea, een internationale en beursgenoteerde onderneming die binnen en buiten Europa opereert als zorgaanbieder. Hierdoor is ook een samenwerking ontstaan op internationaal vlak waarbij kennis en ervaring onderling worden uitgewisseld. Binnen Europa is Allerzorg 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.

De persoonsgegevens worden door een aantal verschillende entiteiten verwerkt. In onderstaand figuur is te zien welke entiteiten de persoonsgegevens verwerken. Het bestuur wordt vanuit Allerzorg Beheer BV gevoerd, waarmee deze entiteit het doel en de middelen van de verwerking van persoonsgegevens vaststelt en daarmee verwerkingsverantwoordelijke is.



4.2. Wijk+

Het cluster Wijk+ bestaat uit een aantal teams die verpleging en persoonlijke verzorging voor volwassenen thuis leveren. Deze teams zijn onderverdeeld in vijf regio's verspreid over Nederland. De regio's worden aangestuurd door een regiomanager, de teams door een teamcoördinator. Het cluster zelf wordt aangestuurd door een divisieleider.

De teams leveren naast verpleging en verzorging ook gespecialiseerde verpleging op het gebied van wondzorg en dermatologie, oncologische zorg en PTZ. De specialistische teams werken samen met ziekenhuizen zodat voor de cliënt het zorgaanbod aansluit op de behoefte. Met deze samenwerkingspartners worden afspraken gemaakt voor het uitwisselen van persoonsgegevens.

4.3. Kind en Gezin

Het cluster Kind en Gezin is opgedeeld in kindzorg, begeleiding en kraamzorg. Kindzorg levert gespecialiseerde verpleging aan kinderen waarbij een vast team van kinderverpleegkundigen bij de zorg voor het kind is betrokken. Hierbij wordt de zorg afgestemd met de ouders en wettelijk vertegenwoordigers. Kindzorg wordt aangestuurd door twee zorgspecialisten die nauw betrokken zijn bij de teams.

Allerzorg levert in een aantal gemeenten gespecialiseerde begeleiding aan gezinnen. Hierbij is vaak sprake van complexe vraagstukken waarbij ook een systeemtherapeut ondersteuning biedt. De teams worden aangestuurd door een zorgspecialist.

Allerzorg Kraamzorg is in regio's onderverdeeld en elke regio wordt aangestuurd door een regiomanager. Tot december 2020 was kraamzorg onderdeel van Allerzorg. In 2020 is de kraamzorg-tak verkocht aan Kraamzorgorganisatie De Waarden.

4.4. Servicebureau

Het servicebureau is in Woerden gevestigd. Binnen het servicebureau worden de bestuurlijke en ondersteunende (bulk)processen uitgevoerd. Hierbij moet worden gedacht aan de directie, de cliëntadministratie, de financiële administratie, HRM, ICT, kwaliteit en directiesecretariaat. Het servicebureau wordt aangestuurd door een directeur bedrijfsvoering.

5. Verwerking van persoonsgegevens

5.1. Beleid

In 2020 is het gegevensbeschermingsbeleid herzien met als doel de wettelijke vereisten die op de verwerking van persoonsgegevens rusten concreet te vertalen naar de uitvoering. In de herziene versie van 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 waar elke medewerker toegang toe heeft.

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 kraamzorg. 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. Allerzorg voldoet 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. Hiermee wordt bedoeld de zorgovereenkomst met de cliënt of de arbeidsovereenkomst met de werknemer. De rechtsgrond van een aantal verwerkingen rust op de noodzaak om aan een wettelijke verplichting te voldoen, bijvoorbeeld om te voldoen 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.

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 Allerzorg gebruik van een ECD[2]. Hierin worden de persoonsgegevens op cliëntniveau gebundeld en gestructureerd. De primaire processen van de organisatie zijn gebaseerd op de gegevens vanuit het ECD. Via regelmatige kwaliteitscontroles wordt vastgesteld of de persoonsgegevens in het ECD juist, volledig en actueel zijn.

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.

[2] Elektronisch cliënten dossier

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 verpleegkundigen en verzorgenden steeds afgewogen of deze gegevens betrekking hebben op het zorgplan die met de cliënt wordt vastgesteld. Wanneer gegevens geen betrekking hebben op dit zorgplan, 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. Eind 2019 heeft Allerzorg archiefbeleid vastgesteld met het doel vast te stellen welke informatie door de organisatie 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 ook op de bedrijfsinformatie.

De implementatie en uitvoering van dit archiefbeleid heeft in 2020 vertraging opgelopen vanwege de ontstane situatie rondom COVID-19. Een deel van de maatregelen zoals in het archiefbeleid is opgenomen worden wel uitgevoerd. Aandacht moet nog wel uitgaan naar de toegang van dossiers van cliënten die niet meer in zorg zijn en werknemers die uit dienst zijn. In de organisatie is nog onvoldoende informatie beschikbaar over de handhaving van de (wettelijke) bewaartermijnen. In 2020 is intern een overzicht van deze termijnen gepubliceerd om de afdelingen hierover te informeren.

5.7. Integriteit en vertrouwelijkheid

Voor het verlenen van de gezondheidszorg zijn gegeven nodig die betrekking hebben op de gezondheid van de cliënten. Deze gegevens moeten vertrouwelijk worden behandeld vanwege het medisch beroepsgeheim wat hierop rust. Deze gegeven zijn opgeslagen in een ECD. Aan dit ECD zijn eisen gesteld ten aanzien van de integriteit van de opgeslagen gegevens. De leverancier is contractueel gebonden om maatregelen te treffen om de integriteit te waarborgen.

Binnen de organisatie worden eisen gesteld aan de toegang tot gegevens in het ECD. Door middel van een autorisatiematrix worden 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 een mobiel apparaat (telefoon of tablet) nodig 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. In 2021 wordt gestart met het systematisch analyseren van deze bestanden zodat kan worden aangetoond dat de toegang tot de gezondheidsgegevens in het ECD rechtmatig is.

6. Beveiligingsmaatregelen

Allerzorg 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 wordt in 2021 geactualiseerd waarbij de normen van NEN7510 als uitgangspunt zijn genomen.

Allerzorg heeft de beschikking over een Information Security Officer (ISO). 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 hij 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. In 2021 worden de beleidsdocumenten, processen en instructies die hierop betrekking hebben binnen de organisatie gepubliceerd.

Er 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 privacy@allerzorg.nl. 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 online register van datalekken.

6.1. Organisatorische maatregelen

De werknemers van Allerzorg 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 2020 is op die manier aandacht gegeven aan het thuiswerken, het op afstand communiceren met cliënten en naasten en het herkennen en omgaan met phishing-berichten.

Papieren gegevensdragers met daarop persoonsgegevens worden in gesloten ruimten opgeslagen zodat zij 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 continu gemonitord. Hierdoor wordt snel ingegrepen wanneer er geprobeerd wordt om onrechtmatig toegang te verkrijgen tot het netwerk en de daarin opgeslagen gegevens. In 2020 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.

In 2020 is een werkinstructie in het handboek gepubliceerd waarin de uitvoering van een DPIA[3] 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 2021 en daarna zal dit principe meer en meer in de organisatie en haar processen moeten worden ingebed.

7.2. Betrokkenheid FG bij nieuwe ontwikkelingen

In 2020 zijn een aantal nieuwe applicaties in gebruik genomen. Hierbij is in de ontwikkeling en implementatie de FG betrokken. Deze betrokkenheid bestaat uit de beoordeling van de ontwikkeling en implementatie van de applicatie in relatie tot de wet- en regelgeving. Voorbeelden hiervan zijn een nieuw rekruteringssysteem, de uitrol van het cliëntportaal, het digitaal ondertekenen van overeenkomsten, een platform voor het verdelen van werk, en de ontwikkeling van een wondzorg-app.

Ook wordt de FG betrokken bij de vorming van samenwerkingsverbanden zoals met het Bravis Ziekenhuis, nachtzorg Flevoland, Medic, het AMC ziekenhuis en Maasstad Ziekenhuis. De betrokkenheid hierbij bestaat uit het ondersteunen bij het maken van afspraken omtrent de verwerking van persoonsgegevens en de wijze waarop deze met de andere partij worden uitgewisseld.

7.3. Uitgevoerde DPIA's

In 2020 zijn twee DPIA's uitgevoerd. In beide gevallen heeft de DPIA geleid tot een verduidelijking van de verwerking van persoonsgegevens, de betrokken partijen en de wettelijke kaders die op deze verwerkingen van toepassing zijn. Ook hebben de DPIA's geleid tot een inzicht in de (mogelijke) risico's voor de rechten en vrijheden van betrokkenen en zijn maatregelen getroffen om deze risico's te minimaliseren.

[3] Data protection impact assessment, ook wel gegevensbeschermingseffectbeoordeling genoemd.

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 Allerzorg verwerkingsverantwoordelijke is. Het register is onderdeel van de verantwoordingsplicht die op Allerzorg rust. Met het register kan Allerzorg 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. Ook bij Allerzorg is dit het geval. In 2020 zijn twaalf (mogelijke) datalekken intern gemeld. Alle meldingen zijn door de FG in behandeling genomen.

In vier gevallen bleek het niet te gaan om een datalek maar om beveiligingsincident waarbij geen inbreuk op persoonsgegevens is geconstateerd.

In vier gevallen bleek dat het datalek waarschijnlijk geen nadelig gevolg heeft voor de betrokkenen. Hierbij moet worden gedacht aan het verkeerd toekennen van rechten met betrekking tot gegevens van een werknemer en het blootgeven van e-mailadressen in e-mail met daarin algemene gegevens. Op basis van deze beoordeling is besloten om – conform de AVG – deze datalekken niet bij de toezichthouder te melden.

In vier gevallen heeft het datalek wel geleid tot een melding bij de toezichthouder. Hierbij is wel sprake geweest van risico's voor de rechten en vrijheden van de betrokkenen. Deze datalekken hebben in de meeste gevallen betrekking op de vertrouwelijkheid van gegevens. In geen van de gevallen is sprake geweest van directe schade van betrokkenen.

9.2. Maatregelen

Alle incidenten die zijn gemeld (of dit nu heeft geleid tot een datalek of niet) hebben wel geleid tot het verbeteren 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. Allerzorg heeft hiervoor een privacyverklaring op haar website gepubliceerd. In 2020 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 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, wissing en gegevensoverdracht. De betrokkene kan zijn rechten bij Allerzorg uitoefenen door een e-mail te sturen naar privacy@allerzorg.nl. Een rechtenverzoek wordt door de FG in ontvangst genomen en binnen de organisatie uitgezet.

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 2020 heeft Allerzorg zes verzoeken van betrokkenen ontvangen. In vijf gevallen is betrokkene binnen een maand geïnformeerd over de afhandeling van het verzoek. In één geval heeft dit zes weken geduurd vanwege de complexiteit van het verzoek. Het ging hierbij om het verstrekken van gezondheidsgegevens na overlijden in het kader van een rechtszaak. In één geval is het verzoek van de verzoeker niet gehonoreerd. Hierbij ging het om verstrekken van gezondheidsgegevens na overlijden aan een nabestaande waarbij het zwaarwegende belang niet kon worden aangetoond.

11. Realisatie ambities 2020

De realisatie van de ambities van 2020 heeft onder druk gestaan van de ontwikkelingen met betrekking tot COVID-19. De prioriteiten werden vanaf het tweede kwartaal vrijwel geheel in beslag genomen om de situatie het hoofd te bieden en om ervoor te zorgen dat zorgverlening kon doorgaan.

11.1. DPIA's

Een van de ambities voor 2020 was om de risico's voor betrokkenen verder te minimaliseren door het uitvoeren van DPIA's waarna aanvullende maatregelen worden getroffen om de toegang en verwerking van persoonsgegevens verder te beveiligen. Zoals eerder aangegeven hebben de prioriteiten van de organisatie zich gericht op de effecten die COVID-19 op de organisatie hebben gehad. Hierbij is geen ruimte geweest om deze geheel doelstelling te realiseren, hoewel wel twee DPIA's zijn uitgevoerd.

11.2. Verantwoording transparanter

In 2019 is een intern normenkader ten aanzien van gegevensbescherming geformuleerd. Met dit normenkader is het toezicht in 2020 vormgegeven en is hierover met de organisatie gecommuniceerd. Het intern normenkader heeft inmiddels plaatsgemaakt voor de Groepsstandaarden van Orpea. Deze standaarden zijn gebaseerd op de wettelijke verplichtingen die rusten de verwerking van persoonsgegevens binnen het concern Orpea. In 2021 worden deze standaarden verder geïmplementeerd en wordt hierover periodiek gerapporteerd aan de Raad van Bestuur.

11.3. Cliëntenportaal

De derde ambitie die Allerzorg in 2019 heeft geformuleerd heeft betrekking op het faciliteren van de rechten van de betrokkenen door het ECD voor een deel open te stellen voor de cliënten. Met dit cliëntportaal heeft de cliënt toegang tot zijn dossier en is het gemakkelijker zijn rechten op diens verwerkte gegevens uit te oefenen. Alle cliënten die verpleging en verzorging ontvangen hebben toegang tot het cliëntportaal.

Cliënten van begeleiding hebben geen toegang tot het cliëntportaal. De hulpverlening is in de meeste gevallen gericht op het systeem (het gezin) waarbij onderlinge relaties complex kunnen zijn. Om te voorkomen dat de inzage in de rapportage leidt tot een inbreuk op de persoonlijke levenssfeer van personen binnen (en buiten) dit systeem leent deze vorm van hulpverlening zich niet voor een cliëntenportaal.

12. Ambities 2021

De onderstaande ambities zijn als beleidsdoelstellingen voor 2021 opgenomen in het gegevensbeschermingsbeleid. Hierover wordt in de verantwoordingsverklaring van 2021 verantwoording afgelegd.

12.1. DPIA verder implementeren

Voor 2021 is deze ambitie opnieuw in de beleidsdoelstellingen opgenomen. Om te voorkomen dat dit beleidsvoornemen opnieuw strand wordt ingezet op een centrale benadering waarbij de FG een meer coördinerende en sturende factor zal zijn in plaats van alleen een adviserende rol in te nemen.

12.2. Bewustwording medewerkers

De bewustwording voor medewerkers is een blijvend aandachtspunt. Naast de opleidingsmodule in de Allerzorg Academie is een programma van bewustwording vastgesteld die gericht op een aantal kernvragen:

- Kennis: wat moet de medewerker weten?
- Houding: wat wordt van de medewerker verwacht?
- Gedrag: doet de medewerker wat van hem/haar wordt verwacht?

De uitvoering is gericht op het onboardingproces (voor nieuwe medewerkers), een thematische benadering van belangrijke onderwerpen en het inspelen op de actualiteit. Kern van het programma vormen de themaweken waarbij onderwerpen als datalekken, wachtwoorden, phishing, bewaartermijnen en de rechten van de betrokkenen centraal staan. De themaweken vormgegeven door blogs van de FG, posters en een quiz.

12.3. Overzicht verbonden partijen

In het gegevensbeschermingsbeleid zijn voor 2021 een aantal beleidsdoelstellingen opgenomen. Een daarvan is het verkrijgen van inzicht en overzicht in de verbonden partijen. Allerzorg maakt deel uit van een groep zorgorganisaties die onder Orpea vallen. In 2021 zal deze groep worden geïntegreerd tot een zorgorganisatie. Tegelijkertijd zijn er zorgorganisaties die door middel van overnames aan de groep worden toegevoegd. Binnen deze dynamiek is het belangrijk om inzicht en overzicht te hebben van de verbonden partijen, zoals entiteiten, verwerkers en samenwerkingspartners.