Verantwoordingsverklaring inzake gegevensbescherming 2018

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

In de Governancecode zorg 2017 is opgenomen dat de Raad van Bestuur verantwoording aflegt over de realisatie van de doelstellingen van de organisatie en het gevoerde beleid ten aanzien van de belanghebbenden. Allerzorg wil transparant zijn in haar handelen en de keuzes die worden gemaakt om daarover vervolgens verantwoording af te leggen aan belanghebbenden.

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 wordt aangetoond. Hiermee wordt een totaalbeeld van 'accountability' gegeven.

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 voor 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 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 2018. 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

Dagelijks wordt door heel Nederland zorg geleverd aan cliënten die hiervan deels of geheel afhankelijk zijn. Om deze zorg goed, veilig en verantwoord te kunnen leveren vragen wij de cliënt naar zijn persoonsgegevens waaronder ook gegevens over de gezondheid. De cliënt vertrouwt erop dat wij integer met deze gegevens omgaan. Dus dat wij niet meer persoonsgegevens verzamelen dan dat nodig is om de zorg te kunnen verlenen, maar ook dat wij ervoor zorgen dat de gegevens goed beveiligd worden zodat zij niet onrechtmatig verwerkt worden en dat de persoonsgegevens niet langer worden bewaard dan noodzakelijk of wettelijk vereist.

Naast de persoonsgegevens van cliënten verzameld en verwerkt Allerzorg ook gegevens van contactpersonen, medewerkers, ZZP-ers, tijdelijk personeel en andere betrokkenen. Ook voor deze gegevens zorgen ervoor wij dat de verwerking ervan rechtmatig en veilig is.

Uitgangspunt van het beleid is dat alleen persoonsgegevens worden verzameld die noodzakelijk zijn om de zorg te verlenen, de gegevens niet langer dan worden bewaard dan nodig is en dat de persoonsgegevens alleen toegankelijk zijn voor diegenen die deze nodig hebben om hun taak uit te voeren. Dit uitgangspunt geldt voor iedereen binnen de organisatie die betrokken is bij de verwerking van persoonsgegevens en vormt de basis van het intern privacy-beleid dat in 2017 is gepubliceerd en geïmplementeerd.

In 2018 is gewerkt aan het ontwikkelen en stimuleren van de bewustwording van de risico's van het werken met persoonsgegevens binnen de organisatie. Daarnaast zijn processen verbetert en systemen aangepast om ervoor te zorgen dat de verwerking van persoonsgegevens veilig en efficiënt verloopt en de betrokkenen worden gefaciliteerd bij het uitoefenen van hun rechten.

Onze ambities voor 2019 moet ervoor zorgen dat gegevensbescherming verder wordt verankerd in de organisatie zodat we onze visie waar kunnen blijven maken en dat we dit kunnen aantonen.

Roy Rempe,

Bestuurder, mei 2019

3. Mededeling Functionaris voor Gegevensbescherming

3.1. Inleiding

Omdat op 25 mei de algemene verordening gegevensbescherming van toepassing werd was 2018 een bijzonder jaar. In aanloop naar deze datum heeft de organisatie geïnvesteerd om zich voor te bereiden op de verplichtingen die deze nieuwe wetgeving met zich meebrengt. In de periode april tot en met september 2018 heb ik door persoonlijke omstandigheden mijn rol als FG niet kunnen invullen. In die periode is de rol van FG ingevuld door de ISO.

Ik heb in oktober 2018 onderzoek gedaan naar de stand van zaken met betrekking tot gegevensbescherming en daarover verslag uitgebracht aan de Raad van Bestuur en Raad van Commissarissen. Op basis daarvan is de conclusie dat Allerzorg in de basis voldoet aan haar verplichtingen die vanuit de AVG op de organisatie van toepassing zijn en dat de meeste beleidsdoelstellingen zijn behaald. Uit het onderzoek blijkt ook dat op het gebied van gegevensbescherming nog verbeteringen kunnen worden doorgevoerd. De punten uit dit onderzoek worden in deze verklaring verder toegelicht.

3.2. Deskundigheid

Om de rol als FG goed te kunnen invullen is deskundigheid nodig van het wettelijke kader waarin persoonsgegevens worden verwerkt, kennis van de praktijk en de techniek waarbinnen de verwerkingen plaatsvinden en adviseert de FG de organisatie om hierover verantwoording af te kunnen leggen. Om deze aspecten van de rol als FG goed te kunnen invullen volg ik via een gespecialiseerd opleidingsinstituut een tweejarige post hbo-opleiding op het gebied van gegevensbescherming. Eind 2019 rond ik deze opleiding af waarna een programma van permanente educatie volgt om op de hoogte te blijven omtrent de ontwikkelingen op het gebied van gegevensbescherming. Hiermee wordt voldaan aan de vereiste dat de FG beschikt over voldoende deskundigheid en competenties om zijn rol goed te kunnen invullen.

3.3. Positionering

De taken en positie van de FG zijn verankerd in de wetgeving. Om de wettelijke taken te vervullen zijn in de aanstellingsbrief van de FG voldoende bevoegdheden opgenomen om deze rol in te kunnen vullen. Door middel van een bestuurlijk overleg rapporteer ik als FG per kwartaal over het intern privacy-beleid rechtstreeks aan de Raad van Bestuur. Door de eerder genoemde persoonlijke omstandigheden heeft dit overleg in 2018 slechts tweemaal plaatsgevonden.

Buiten dit overleg adviseer ik gevraagd en ongevraagd de organisatie over gegevensbescherming en ben ik betrokken bij het afhandelen van incidenten.

Frans Schreuder,

functionaris voor gegevensbescherming, mei 2019

4. Organisatiebeschrijving en bescherming persoonsgegevens

4.1. Organisatiebeschrijving

Als landelijke aanbieder van thuiszorg werkt Allerzorg met teams die (gespecialiseerde) verpleging, verzorging, begeleiding en kraamzorg thuis bij de cliënt leveren. De teams werken op basis van uniforme kwaliteitsstandaarden en protocollen. Allerzorg heeft deze teams in specialismen georganiseerd zodat hoogwaardige zorg kan worden geleverd. Het betreft wijkverpleging, palliatief terminale zorg, wondzorg en dermatologie, specialistische zorg, kraamzorg, kindzorg en begeleiding.

De teams worden vanuit het centraal kantoor in Woerden ondersteund door een aantal stafafdelingen. Deze stafafdelingen leveren diensten aan de teams zodat zij zich kunnen richten op het verlenen van goede, veilige en verantwoorde zorg. De specialismen en stafafdelingen worden aangestuurd door de Raad van Bestuur.

Om de zorg te kunnen plannen, verlenen en verantwoorden werken de teams met een ECD[2]. Dit geldt niet voor de specialismen kraamzorg en begeleiding. De zorg van deze specialismen wordt in een papieren dossier geregistreerd en verantwoord, waarbij het de bedoeling is om ook deze specialismen in de nabije toekomst op een ECD aan te sluiten.

Om met het ECD te kunnen werken en contact te kunnen hebben met de organisatie beschikt elke medewerker over een door de organisatie uitgegeven smartphone. De toegang tot de smartphone is beveiligd, evenals de verbinding met het ECD. De informatie en documentatie van de organisatie kan worden benaderd via een Azure Active Directory (AAD) die toegang geeft tot het ECD, Office365-omgeving, intranet, academie en documentmanagementsysteem.

4.2. Bescherming persoonsgegevens

Uitgangspunt is dat degene die verantwoordelijk is voor een proces waarin persoonsgegevens worden verwerkt, ook verantwoordelijk is voor de betreffende verwerkingen. De eigenaren zijn in het register van verwerkingsactiviteiten gekoppeld aan de verwerkingen. In geval van incidenten, vragen of onderzoeken worden de eigenaren betrokken om hierop te reageren.

4.2.1. Driehoek

De gegevensbescherming is binnen de organisatie in een zogenaamde ‘driehoek’ vormgegeven. Deze driehoek is samengesteld uit de informatie manager, ISO en FG. Tenminste eenmaal per twee weken vindt een overleg plaats waarin de uitvoering van de intern privacy-beleid en het informatiebeveiligingsbeleid wordt besproken. Doel van het overleg is om vast te stellen in hoeverre de getroffen technische en organisatorische beveiligingsmaatregelen effectief zijn en welke aanvullende maatregelen moeten worden getroffen om de effectiviteit ervan te verbeteren.

In het overleg komen onder andere de meldingen van incidenten, getroffen technische en organisatorische beveiligingsmaatregelen, ontwikkelingen ten aanzien van de organisatie, techniek en wet- en regelgeving en projecten gerelateerd aan gegevensbescherming aan de orde. De besluiten en actiepunten van het overleg worden vastgelegd.

[2] Elektronisch cliëntendossier

4.2.2. Continue monitoring

De toegang tot de primaire systemen en dataopslag vindt plaats via de AAD. De toegang via de AAD wordt continu gemonitord waarmee inzicht wordt verkregen in wie toegang heeft tot de primaire systemen en dataopslag. De anomalieën betreffende de toegang worden binnen Azure gesignaleerd en op basis hiervan gaat de ISO na of deze signalen (kunnen) leiden of hebben geleid tot onrechtmatige toegang. De instrumenten om deze anomalieën te signaleren worden continu geüpdatet. De anomalieën worden besproken in de driehoek indien daartoe aanleiding is en eventueel worden (aanvullende) maatregelen getroffen om kwetsbaarheden op te lossen of bedreigingen het hoofd te bieden.

4.2.3. Incidentmanagement

Incidenten met betrekking tot de verwerking van persoonsgegevens worden centraal gemeld en vastgelegd in het incidentregister. Een incident in verband met persoonsgegevens kan door elke medewerker op verschillende manieren worden gemeld. Bij de afhandeling van elke melding is zowel de FG als ISO betrokken. In 2018 zijn zestien incidenten gemeld en vastgelegd, waarbij dit in één geval heeft geleid tot een melding van een datalek.

Uit de oorzakenanalyse van de incidentmeldingen blijkt dat de meeste incidenten worden veroorzaakt door gestolen of zoekgeraakte mobiele apparatuur zoals smartphones en laptops. De opslag van deze apparatuur is standaard versleuteld en de betrokken apparaten worden van afstand gewist zodat wordt voorkomen dat persoonsgegevens onrechtmatig worden verwerkt.

4.2.4. Awareness

In 2018 zijn een aantal sessies geweest om het management bewust te maken van de nieuwe wetgeving (de AVG) en hun verantwoordelijkheden hierin. Deze sessies zijn gegeven door de FG en de ISO. Tijdens deze sessies is het management bewust gemaakt wat gegevensbescherming inhoudt en wat hún rol is bij het beschermen van persoonsgegevens.

Om gegevensbescherming dichter bij de teams te brengen zijn een aantal aandachtfunctionarissen benoemd. Deze functionarissen hebben als rol om vragen van teamleden te beantwoorden, nieuwe ontwikkelingen onder de aandacht van de teams te brengen, incidenten op te vangen en bijzonderheden ten aanzien van gegevensbescherming te signaleren. Hiervoor zijn de functionarissen gedurende twee dagdelen door de FG opgeleid.

In de maanden mei tot en met september 2018 heeft de ISO middels een aantal nieuwsberichten aandacht gevraagd voor het onderwerp informatiebeveiliging. Hierbij was bijvoorbeeld het gebruik van WhatsApp, het voorkomen van phishing en het veilig omgaan met persoonsgegevens het onderwerp.

In juni 2018 hebben studenten van de Haagse Hogeschool in opdracht van Allerzorg een phishingactie uitgevoerd om de weerbaarheid van Allerzorg te testen. Het doel was tweeledig: enerzijds het testen van onze digitale systemen en processen, aan de andere kant het bewustzijn van de medewerkers op de proef stellen.

De test is als volgt uitgevoerd: een aantal medewerkers ontving een e-mail die afkomstig leek van Xantion, onze partner in ICT-ondersteuning. In de e-mail werd uitgenodigd om op een link te klikken. Meer dan de helft heeft op de link geklikt en twee medewerkers hebben de helpdesk gebeld. Naar aanleiding hiervan zijn opnieuw nieuwsberichten verstuurd om medewerker bewust te maken van phishing.

5. Beleid

De Raad van Bestuur heeft eind 2017 het intern privacy-beleid en het informatiebeveiligingsbeleid vastgesteld. Deze beleidsdocumenten vormen de basis voor gegevensbescherming binnen de organisatie.

5.1. Uitgangspunten

In het verlengde van de visie van de organisatie: '*zorg zoals je voor je naasten wenst*', zijn de uitgangspunten voor het verwerken van persoonsgegevens in het privacy-beleid vastgesteld. Hierbij wordt een evenwicht gezocht tussen het verlenen van goede, veilige en verantwoorde zorg en het veilig en verantwoord verwerken van persoonsgegevens:

- Privacy en gegevensbescherming mag de zorgverlening niet in de weg staan.
- Evenwicht tussen gebruikersgemak en gegevensbescherming.
- Uitgangspunt is vertrouwen in de professionaliteit van de medewerker, maar er vindt wel controle plaats (auditability).
- Zorgvuldigheid staat voorop maar het uitsluiten van datalekken is niet mogelijk.

Naast de bovengenoemde uitgangspunten heeft het van toepassing worden van de AVG in mei 2018 tot de volgende beleidsdoelstellingen van 2018 geleid:

- Het systematisch in beeld brengen van de verwerkingen van persoonsgegevens;
- Het creëren van inzicht en overzicht in de verantwoordelijkheden en aansprakelijkheden;
- Het maken van afspraken met verwerkers en andere partijen die betrokken zijn bij de verwerkingen van persoonsgegevens;
- Het faciliteren van de rechten van betrokkenen, zowel de actieve als de passieve rechten;
- De betrokkene is in control over de verwerking van zijn persoonsgegevens.

5.2. Realisatie

Het grootste deel van de beleidsdoelstellingen zijn behaald. De verwerkingen van persoonsgegevens zijn opgenomen in een centraal register. Hiermee wordt tevens voldaan aan de wettelijke verplichting om een dergelijk register te voeren.

Het maken van afspraken met andere partijen die betrokken zijn bij de verwerkingen van persoonsgegevens is een continuproces omdat Allerzorg als landelijke zorgaanbieder met veel verschillende partijen samenwerkt om goede zorg te kunnen verlenen. Het maken van afspraken met deze partijen is in bepaalde gevallen een complexe aangelegenheid omdat over de verantwoordelijkheden en aansprakelijkheden moet worden onderhandeld.

Voor het maken van afspraken met verwerkers gaat Allerzorg uit van de standaardovereenkomst die de BOZ[3] wordt gehanteerd. In 2019 wordt ingezet om het contractbeheer verder te professionaliseren zodat ook het inzicht en overzicht van de verantwoordelijkheden en aansprakelijkheden verbeterd wordt.

Om de betrokkenen te informeren over de verwerking van hun persoonsgegevens en hun rechten hierin heeft Allerzorg een privacyverklaring gepubliceerd. In de verklaring wordt ingegaan op de aard van de verwerking, de doeleinden, de grondslagen, bewaartermijnen en ontvangers van

[3] Brancheorganisaties in de zorg

persoonsgegevens. Daarnaast wordt ingegaan op welke rechten de betrokkene heeft en op welke wijze en onder welke voorwaarden deze rechten kunnen worden uitgeoefend.

Om de betrokkene in control te brengen over de verwerking van zijn persoonsgegevens is het noodzakelijk dat de betrokkene via een portal kan inloggen in het ECD. Hiermee kan de betrokkene inzicht verkrijgen in de verwerking van zijn persoonsgegevens, wijzigingen en rectificaties kan doorgeven en daarnaast – indien de verwerking is gebaseerd op toestemming – de toestemming verlenen of intrekken. Het bedoelde portal is nog niet operationeel zodat voorgenoemde inzicht en beheer nog niet is gerealiseerd.

6. Verwerkingen van persoonsgegevens

Voor de primaire en ondersteunende processen worden persoonsgegevens vastgelegd van diverse categorieën betrokkenen. Voor de cliënten (zorgvragers) worden daarnaast ook gezondheidsgegevens vastgelegd om de zorgvraag te kunnen beoordelen, plannen, verlenen, evalueren en verantwoorden. Dit betreft ook betrokkenen die vanwege hun leeftijd, aandoening, beperkingen of gezondheidstoestand kwetsbaar zijn.

6.1. Overzicht van doeleinden van verwerkingen

In onderstaande tabel zijn per hoofdproces de doeleinden voor de verwerkingen van persoonsgegevens in relatie tot de betrokkenen opgenomen.

Hoofdproces	Doeleinde	Betrokkenen
Beheer bedrijfsmiddelen	Het aanvragen, gebruiken, onderhouden en inleveren van een leaseauto.	Medewerker; PNIL-er[4]
Beheer bedrijfsmiddelen	Het aanvragen, gebruiken en inleveren van een smartphone.	Medewerker; PNIL-er
Financiële administratie	Het in behandeling nemen en afhandelen van schademeldingen.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Medewerker; PNIL-er
Financiële administratie	Het declareren van de zorgverlening bij de uitvoerder (Zwv, Wlz of Wmo).	Cliënt; Zorgvrager
Financiële administratie	Het voeren van een debiteuren- en crediteurenadministratie.	Cliënt; PNIL-er
Financiële administratie	Het voeren van een cliëntenadministratie ten behoeve van het ophalen van indicaties en het verzenden van declaraties.	Cliënt; Zorgvrager
Gratificaties	Het bestellen en uitgeven van kerstpakketten.	Medewerker
Klachten en geschillen	Het afhandelen van klachten en geschillen.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Klager
Kwaliteitsverbetering	Het certificeren/accrediteren van het kwaliteitssysteem en de organisatie.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Klager; Medewerker; PNIL-er; Vrijwilliger; Sollicitant
Kwaliteitsverbetering	Het verzamelen, analyseren, beoordelen van de tevredenheid van de cliënt omtrent de zorg-	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger

[4] Personeel niet in loondienst, zoals een zelfstandige zonder personeel, uitzendkracht, vrijwilliger, etc.

Hoofdproces	Doeleinde	Betrokkenen
	en dienstverlening teneinde de kwaliteit van de zorg- en dienstverlening te verbeteren.	
Kwaliteitsverbetering	Het inventariseren, onderzoeken, analyseren en rapporteren van incidenten en calamiteiten in de zorgverlening.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Medewerker; PNIL-er; Vrijwilliger
Kwaliteitsverbetering	Het verbeteren van de zorg- en dienstverlening.	Cliënt; Zorgvrager
Kwaliteitsverbetering	Het beperken van de gevolgen van een incident, het voorkomen van incidenten en het verbeteren van de zorg- en dienstverlening.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Medewerker; PNIL-er; Vrijwilliger
Opleidingen	Het verzamelen, beoordelen, evalueren en vastleggen van competenties.	Medewerker; PNIL-er
Opleidingen	Het opleiden, bijscholen en trainen van medewerkers en PNIL-ers.	Medewerker; PNIL-er
Personeelsadministratie	Het archiveren van het papieren deel van het personeelsdossier.	Medewerker
Personeelsadministratie	Het werven en selecteren van nieuwe medewerkers.	Medewerker; Sollicitant
Personeelsadministratie	Het werven en selecteren van personeel niet in loondienst (PNIL).	PNIL-er
Salarisadministratie	Het berekenen en afdragen van pensioenpremie van medewerkers.	Medewerker
Salarisadministratie	Het berekenen en betalen van salaris aan medewerkers.	Medewerker
Systeembeheer	Het verstrekken, beheren en intrekken van toegang tot informatiesystemen.	Medewerker; PNIL-er
Systeembeheer	Het vaststellen, beoordelen, evalueren en aanpassen van de werking van informatiesystemen.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Klager; Medewerker; PNIL-er; Vrijwilliger; Sollicitant
Systeembeheer	Het routeren en volgen van het ingaande en uitgaande telefoonverkeer.	Beller

Hoofdproces	Doeleinde	Betrokkenen
Systeembeheer	Het routeren en volgen van bezoekers van de website, het vergroten van het gebruikersgemak en het beantwoorden van specifieke vragen.	Bezoeker website
Systeembeheer	Het ondersteunen van gebruikers bij het gebruik van hard- en software.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Klager; Medewerker; PNIL-er; Vrijwilliger; Sollicitant
Verantwoording	Het verzamelen en beheren van toestemming van het leveren van persoonsgegevens aan de CCR[5] ten behoeve van het cliënttevredenheidsonderzoek door de CCR.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger
Verantwoording	Het voldoen aan de wettelijke meldplicht.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Medewerker; PNIL-er; Vrijwilliger
Verzuimbegeleiding	Het voeren van een verzuimadministratie t.b.v. de re-integratie van verzuimers en voldoen aan wet Poortwachter.	Medewerker
Zorgverlening Kraamzorg	Het beoordelen van de zorgvraag van een zorgvrager om te bepalen of de zorgvraag in zorg genomen kan worden.	Cliënt; Zorgvrager
Zorgverlening Kraamzorg	Het vaststellen van de identiteit van de zorgvrager, het informeren van de zorgvrager over de kraamzorg en het opvragen van informatie over de wensen en behoeften en de woningkenmerken.	Cliënt; Zorgvrager
Zorgverlening Kraamzorg	Het vaststellen van de status van ziektekostenverzekering en het verzamelen en vastleggen van de polisgegevens ten behoeve van de declaratie kraamzorg.	Zorgvrager
Zorgverlening Kraamzorg	Het vaststellen van de geldigheid van het identiteitsbewijs.	Zorgvrager
Zorgverlening Kraamzorg	Het inventariseren van de contactgegevens van de contactpersoon van de zorgvrager zodat deze in een spoed- of noodsituatie kan worden ingelicht.	Contactpersoon
Zorgverlening Kraamzorg	Het plannen van de kraamzorg.	Cliënt; Zorgvrager

[5] Centrale cliëntenraad

Hoofdproces	Doeleinde	Betrokkenen
Zorgverlening Kraamzorg	Het verlenen en evalueren van de kraamzorg.	Cliënt; Zorgvrager
Zorgverlening Kraamzorg	Het afsluiten van de zorgverlening en het evalueren van de tevredenheid van de kraamzorg.	Cliënt; Zorgvrager
Zorgverlening Kraamzorg	Het overdragen van informatie uit het kraambed naar JGZ.	Cliënt; Zorgvrager; Pasgeborene
Zorgverlening Kraamzorg	Het archiveren van de templijst en evaluatieformulier.	Cliënt; Zorgvrager; Pasgeborene
Zorgverlening Kraamzorg	Het verstrekken van informatie ten behoeve van het mogelijk maken van een detailcontrole om de rechtmatigheid en de betrouwbaarheid van de zorgdeclaraties aan te tonen.	Cliënt; Zorgvrager; Pasgeborene
Zorgverlening Kraamzorg	Het melden van signalen van kindermishandeling of huiselijk geweld ten behoeve van het verlenen van hulp.	Cliënt; Zorgvrager
Zorgverlening V&V	Het verstrekken van informatie over de zorgvraag in het kader van de overdracht aan een andere zorgaanbieder.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger
Zorgverlening V&V	Het verstrekken van informatie ten behoeve van het mogelijk maken van een detailcontrole om de rechtmatigheid en de betrouwbaarheid van de zorgdeclaraties aan te tonen.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger; Medewerker; PNIL-er
Zorgverlening V&V	Het aannemen, uitvoeren, evalueren en vastleggen van voorbehouden handelingen.	Zorgvrager
Zorgverlening V&V	Het vaststellen van de status van ziektekostenverzekering en het verzamelen en vastleggen van de polisgegevens ten behoeve van de declaratie zorgverlening.	Zorgvrager
Zorgverlening V&V	Het vaststellen van de geldigheid van het identiteitsbewijs.	Cliënt; Zorgvrager
Zorgverlening V&V	Het archiveren van het papieren zorgdossier.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Vrijwilliger
Zorgverlening V&V	Het archiveren van het ECD.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Vrijwilliger
Zorgverlening V&V	Het vaststellen, vastleggen en evalueren van de indicatie wijkverpleging.	Zorgvrager
Zorgverlening V&V	Het controleren van de medicatie, het toedienen en evalueren van medicatie en het vastleggen van de toediening.	Zorgvrager

Hoofdproces	Doeleinde	Betrokkenen
Zorgverlening V&V	Het verlenen van toegang tot het ECD en Kompas	PNIL-er
Zorgverlening V&V	Het beoordelen van de zorgvraag van een zorgvrager om te bepalen of de zorgvraag in zorg genomen kan worden.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid
Zorgverlening V&V	Het vaststellen van de identiteit van de zorgvrager, uitvoeren van een intake, afsluiten zorgovereenkomst, het vaststellen van de indicatie van de zorgvraag en het opstellen en bespreken van het zorgplan.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger; Familielid
Zorgverlening V&V	Het inventariseren van de contactgegevens van de contactpersoon van de zorgvrager zodat deze in een spoed- of noodsituatie kan worden ingelicht.	Contactpersoon
Zorgverlening V&V	Het inplannen van de zorgverlening.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Familielid
Zorgverlening V&V	Het verlenen van zorg en het periodiek evalueren van de zorgverlening.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger
Zorgverlening V&V	Het inventariseren en verlenen van nazorg.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger
Zorgverlening V&V	Het afsluiten van de zorgverlening en het archiveren van het zorgdossier.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger
Zorgverlening V&V	Het archiveren van het papieren deel van het zorgdossier.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid
Zorgverlening V&V	Het bieden van telefonische bereikbaarheid buiten kantoortijden.	Cliënt; Zorgvrager; Mantelzorger; Wettelijk vertegenwoordiger; Contactpersoon; Familielid; Vrijwilliger
Zorgverlening V&V	Het dubbel controleren van risicovolle medicatie en het vastleggen van de dubbele controle.	Cliënt; Zorgvrager; Medewerker; PNIL-er

Hoofdproces	Doeleinde	Betrokkenen
Zorgverlening V&V	Het verzamelen en beoordelen van informatie over de zorgvraag in het kader van de overdracht van een andere zorgaanbieder.	Cliënt; Zorgvrager; Wettelijk vertegenwoordiger

6.2. Beheersmaatregelen

De organisatie heeft op een aantal vlakken beheersmaatregelen getroffen om hiervoor genoemde verwerkingen van persoonsgegevens te beveiligen. Met verwerkers is middels een verwerkersovereenkomst overeengekomen dat hun dienstverlening tenminste voldoet aan de hieronder gestelde eisen.

6.2.1. Organisatie van informatiebeveiliging en communicatieprocessen

- De verwerking van persoonsgegevens is onderworpen aan het informatiebeveiligingsbeleid;
- Er is een ISO aangesteld om de risico's met betrekking tot de verwerking van persoonsgegevens te inventariseren, voorzieningen te controleren, beveiligingsbewustzijn te stimuleren en maatregelen te treffen die toezien op de naleving van het informatiebeveiligingsbeleid;
- Er is een proces ingericht voor het communiceren over incidenten met betrekking tot de verwerking van persoonsgegevens;
- Op nieuwe en bestaande verwerkingen, wordt – indien hiertoe aanleiding is – een DPIA uitgevoerd om de risico's voor betrokkenen te inventariseren en maatregelen te treffen om deze risico's te minimaliseren of te beperken;
- Incidenten worden gedocumenteerd en worden gebruikt om de verwerking en beveiliging van persoonsgegevens te optimaliseren.

6.2.2. Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt;
- De medewerkers worden gestimuleerd in het bewustzijn ten aanzien van informatiebeveiliging, indien nodig worden de medewerkers verder opgeleid en getraind;
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

6.2.3. Fysieke beveiliging en continuïteit van de middelen

- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.

- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's. Met verwerkers is overeengekomen dat deze beschikt over bedrijfscontinuïteitsplannen waarin uitwijklocaties zijn opgenomen.

6.2.4. Netwerk-, server- en applicatiebeveiliging en onderhoud

- De netwerkomgeving waarbinnen gegevens worden verwerkt strikt is beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- De digitale systemen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie. En dat wijzigingen in applicaties worden getest op kwetsbaarheden voordat deze in productie worden genomen.
- Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd op basis van patchmanagement.
- Penetratietests en vulnerability assessments worden periodiek uitgevoerd.
- Niet (meer) gebruikte informatie wordt verwijderd.
- Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- Er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen.

7. Onderzoeken

Naar aanleiding van het voornemen om een cliëntportal in te richten en open te stellen voor cliënten en mantelzorgers is in januari 2018 een onderzoek uitgevoerd op de risico's die dit voor betrokkenen met zich mee brengt. De uitkomst van dit onderzoek heeft geleid tot het uitstellen van de inrichting van het portal totdat het ontwerp en implementatie voldoende garanties biedt voor een veilige verwerking van persoonsgegevens.

In oktober 2018 is een onderzoek uitgevoerd op de stand van zaken ten aanzien van de gegevensverwerkingen binnen de organisatie. In november 2018 is aan de Raad van Bestuur een rapport verstrekt.

De belangrijkste uitkomsten zijn dat in de aanloop van het van toepassing worden van de AVG en daarna veel aandacht is geweest voor het onderwerp gegevensbescherming en de eisen die de wetgeving hieraan stelt. Er zijn maatregelen getroffen om uitvoering te geven aan het intern privacy-beleid en informatiebeveiligingsbeleid. In het onderzoek zijn een aantal aanbevelingen opgenomen. De belangrijkste aanbevelingen betreffen:

- Het verbeteren van de informatievoorziening aan de FG vanuit het management betreffende de ontwikkelingen die samenhangen met de verwerking van persoonsgegevens;
- Het verder in kaart brengen van de gegevensuitwisseling met derde partijen (verwerkers, gezamenlijk verantwoordelijken en andere verwerkingsverantwoordelijken);
- Het inrichten van een doorlopend programma van bewustwording in het kader van gegevensbescherming.

De Raad van Bestuur heeft deze aanbevelingen overgenomen. De belangrijkste onderwerpen worden geagendeerd voor het kwartaaloverleg tussen Raad van Bestuur en FG met als doel de voortgang ervan te monitoren.

8. Ambities voor 2019

Allerzorg heeft de ambitie om het behaalde volwassenheidsniveau te consolideren en in 2019 verder te verhogen. Hiervoor worden de huidige doelstellingen herijkt en nieuwe doelen gesteld. Deze herijking is doorgevoerd in het intern privacy-beleid. De doelstellingen voor 2019 zijn als volgt geformuleerd:

- Gegevensbescherming en privacy zijn ingebouwd in de organisatie. Niet alleen in de informatiesystemen, maar ook in het handelen van medewerkers, ZZP-ers en leveranciers.
- De effectieve werking van getroffen maatregelen en mechanismen kan worden aangetoond. Allerzorg is accountable en gegevensbescherming is verankerd in de bedrijfsvoering. Het is onderdeel van het risicomanagement en een verplicht onderdeel van de jaarrekening.
- Medewerkers en ZZP-ers zijn zich bewust van de risico's die het verwerken van persoonsgegevens voor betrokkenen heeft op hun rechten en vrijheden. De betrokkene is in control over de verwerking van zijn persoonsgegevens.

Om hieraan uitvoering te geven wordt:

- het verzamelen en analyseren van verantwoordingsinformatie verder ontwikkeld tot een dashboard van waaruit verantwoording kan worden afgelegd;
- het bewustwordingsprogramma als continuproces ingericht;
- het cliëntenportal operationeel zodat betrokkenen verder worden gefaciliteerd worden in de uitoefening van hun rechten;
- het beleid contractbeheer en de samenhangende processen en systemen herijkt ingericht.
- het archiefbeleid en de daarmee samenhangende processen en systemen herijkt.

De doelstellingen zijn onderdeel van de agenda van het kwartaaloverleg tussen Raad van Bestuur en de FG.