Verantwoordingsverklaring inzake gegevensbescherming 2019

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

Inhoudsopgave

1. Inleiding 3
   1.1. Doel Verklaring 3
   1.2. Gebruik van de verklaring 3
2. Mededeling Raad van Bestuur 4
3. Mededeling Functionaris voor Gegevensbescherming 5
   3.1. Inleiding 5
   3.2. Deskundigheid 5
   3.3. Positionering 5
4. Organisatiebeschrijving 6
5. Overzicht van doeleinden van verwerkingen 7
6. Framework 9
   6.1. Wet- en regelgeving, normen en beleid 9
   6.2. Handelen en gedrag 10
   6.3. Technische en fysieke beveiliging 10
7. Analyse datalekken 12
8. Ambities voor 2020 13

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 worden zij ondersteund door de informatiemanager (verschaft techniek), FG (adviseert o.g.v. wetgeving en de praktijk) en 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 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 2019. 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 en zijn naasten vertrouwen 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 ons 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 gegevensbeschermingsbeleid.

De uitvoering van dit beleid is onderhevig aan interne en externe ontwikkelingen. Hierbij gaat het om de tarieven en contractvolumes die in de gezondheidszorg onder druk staan, overnames van bestaande zorgaanbieders, de toenemende digitalisering van processen, de bedreigingen vanuit de digitale wereld en betrokkenen die zich steeds meer bewust zijn van hun rechten. Daarnaast hebben we te maken met veranderende wetgeving en de aanscherping van wensen en behoeften van de stakeholders in relatie tot de gegevensverwerkingen.

In 2019 is Allerzorg gegroeid door overnames en is onderdeel geworden van Orpea, een internationaal opererende zorgaanbieder. Daarnaast werkt Allerzorg nauw samen met Wonen bij September wat ook onderdeel is van Orpea. Met de groeiende organisatie wordt gebruik gemaakt van de schaalvergroting en hiermee worden de processen verder gedigitaliseerd. Deze digitalisering zorgt ervoor dat de risico's voor betrokkenen kunnen toenemen indien deze onrechtmatig worden verwerkt. Vandaar dat onze ambities zijn gericht op het verder beveiligen van de gegevens, het faciliteren van de rechten van betrokkenen en het transparanter maken van de verwerking van de persoonsgegevens.

Onze ambities voor 2020 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

Loïc Batesti
Bestuurder

April 2020

3. Mededeling Functionaris voor Gegevensbescherming

3.1. Inleiding

In 2019 is Allerzorg onderdeel geworden van Orpea, een internationale en beurgenoteerde onderneming die binnen en buiten Europa opereert. Deze verandering heeft tot gevolg dat er een samenwerking is ontstaan met andere FG's van onderdelen van Orpea uit andere landen. Gezien het internationale karakter biedt dit naast nieuwe inzichten ook voordelen in het delen van vraagstukken en oplossingen.

Daarnaast zijn er nog andere veranderingen zoals de software voor de privacy-administratie die vanuit Orpea wordt aangeboden door middel van een webapplicatie, het maandelijks overleg met de FG van Orpea Groep en het bijwonen van workshops en trainingen.

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. Hiervoor heb ik in 2019 een tweejarige post hbo-opleiding op het gebied van gegevensbescherming met een positief resultaat afgerond via Duthler Academy. Vanaf 2020 blijf ik een programma van permanente educatie volgen om op de hoogte te blijven omtrent de ontwikkelingen op het gebied van gegevensbescherming. Daarnaast ben ik lid van een aantal werkgroepen en ga ik naar bijeenkomsten en congressen waar gegevensbescherming centraal staat. 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 gegevensbeschermingsbeleid rechtstreeks aan de Raad van Bestuur.

Als FG werk ik nauw samen met de informatiemanager en ISO. Eenmaal per twee weken vindt overleg plaats waarbij gegevensbescherming en informatiebeveiliging op de agenda staat. Buiten de overlegstructuren adviseer ik gevraagd en ongevraagd de organisatie over gegevensbescherming en ben ik betrokken bij het afhandelen van incidenten.

Frans Schreuder
Functionaris voor gegevensbescherming

April 2020

4. Organisatiebeschrijving

Als landelijke aanbieder van zorg thuis werkt Allerzorg met teams die (gespecialiseerde) verpleging, verzorging, begeleiding en kraamzorg thuis bij aan cliënten 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, palliatieve terminale zorg, wondzorg en dermatologie, verpleegtechnische zorg, kraamzorg, medische kindzorg en specialistische 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 specialistische 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.

[2] Elektronisch cliëntendossier

5. Overzicht van doeleinden van verwerkingen

Ten behoeve van de uitvoering van de zorgovereenkomst en op grond van contractuele en wettelijke verplichtingen worden van cliënten, wettelijk vertegenwoordigers en contactpersonen van cliënten de voor de volgende doeleinden persoonsgegevens verwerkt:

- Het beoordelen van de zorgvraag van een zorgvrager om te bepalen of de zorgvraag in zorg genomen kan worden.
- Het vaststellen van de status van ziektekostenverzekering en het verzamelen en vastleggen van de polis gegevens ten behoeve van de declaratie zorgverlening.
- 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.
- Het vaststellen van de geldigheid van het identiteitsbewijs.
- Het vaststellen, vastleggen en evalueren van de indicatie wijkverpleging.
- Het inplannen van de zorgverlening.
- Het inventariseren van de contactgegevens van de contactpersoon van de zorgvrager zodat deze in een spoed- of noodsituatie kan worden ingelicht.
- Het aannemen, uitvoeren, evalueren en vastleggen van voorbehouden handelingen.
- Het controleren van de medicatie, het toedienen en evalueren van medicatie en het vastleggen van de toediening.
- Het verlenen van zorg en het periodiek evalueren van de zorgverlening.
- Het verlenen van zorg onder gezamenlijke verantwoordelijkheid of in samenwerking met andere zorgaanbieders.
- Het bieden van telefonische bereikbaarheid buiten kantoortijden.
- Het certificeren/accrediteren van het kwaliteitssysteem en de organisatie.
- Het verzamelen, analyseren, beoordelen van de tevredenheid van de cliënt omtrent de zorg- en dienstverlening teneinde de kwaliteit van de zorg- en dienstverlening te verbeteren.
- Het beperken van de gevolgen van een incident, het voorkomen van incidenten en het verbeteren van de zorg- en dienstverlening.
- Het inventariseren, onderzoeken, analyseren en rapporteren van incidenten en calamiteiten in de zorgverlening.
- Het afhandelen van klachten en geschillen.
- Het melden van signalen van kindermishandeling of huiselijk geweld ten behoeve van het verlenen van hulp.
- 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.
- Het inventariseren en verlenen van nazorg.
- Het beheren van het archief.
- Het voeren van een cliëntenadministratie ten behoeve van het ophalen van indicaties en het verzenden van declaraties.
- Het declareren van de zorgverlening bij de uitvoerder (Zwv, Wlz, Wmo en Jeugdwet).
- Het voeren van een debiteuren- en crediteurenadministratie.
- Het in behandeling nemen en afhandelen van schademeldingen.

- Het vaststellen, beoordelen, evalueren en aanpassen van de werking van informatiesystemen.
- Het routeren en volgen van het ingaande en uitgaande telefoonverkeer.
- Het routeren en volgen van bezoekers van de website, het vergroten van het gebruikersgemak en het beantwoorden van specifieke vragen.
- Het verzamelen en beoordelen van informatie over de zorgvraag in het kader van de overdracht van een andere zorgaanbieder.

Ten behoeve van de uitvoering van de arbeidsovereenkomst of overeenkomst tot opdracht en op grond van contractuele en wettelijke verplichtingen worden van medewerkers en PNIL-ers[3] en contactpersonen van medewerkers de voor de volgende doeleinden persoonsgegevens verwerkt:

- Het werven en selecteren van nieuwe medewerkers en PNIL-ers.
- Het verstrekken, beheren en intrekken van toegang tot informatiesystemen.
- Het aanvragen, gebruiken en inleveren van een smartphone.
- Het aanvragen, gebruiken, onderhouden en inleveren van een leaseauto.
- Het aanvragen, ontvangen en bewaren van Verklaringen omtrent het gedrag (VOG)
- Het verzamelen, beoordelen, evalueren en vastleggen van competenties.
- Het opleiden, bijscholen en trainen van medewerkers en PNIL-ers.
- Het berekenen en betalen van salaris aan medewerkers.
- Het berekenen en afdragen van pensioenpremie van medewerkers.
- Het afhandelen van loonbeslagen
- Het aanvragen en verantwoorden van subsidieregelingen
- Het vaststellen, beoordelen, evalueren en aanpassen van de werking van informatiesystemen.
- Het bestellen en uitgeven van kerstpakketten.
- Het regelen van ontslag en, indien van toepassing, het regelen van uitkeringen in verband met de beëindiging van een dienstverband
- Het beheren van het archief.
- Het routeren en volgen van het ingaande en uitgaande telefoonverkeer.
- Het voeren van een verzuimadministratie t.b.v. de re-integratie van verzuimers en voldoen aan wettelijke verplichtingen.

[3] Personeel niet in loondienst

6. Framework

Hieronder is het framework weergegeven waarbinnen gegevensbescherming en informatiebeveiliging is georganiseerd en van waaruit verantwoording wordt afgelegd.

Framework	Wet- en regelgeving, normen en beleid	Handelen en gedrag	Technische en fysieke beveiliging
Gegevensbescherming en informatiebeveiliging	Wet- en regelgeving Beroeps- en gedragdcodes NEN-normen Beleidsdocumenten Protocollen Werkinstructies	Bewustwording Presentaties Trainingen Informeren	Functioneel applicatiebeheer Melden incidenten
Monitoring en controle	Monitoring wet- en regelgeving Evalueren proces In- en externe audits en onderzoeken Datalek analyse	Monitoren gedrag en naleven regels Evalueren proces In- en externe audits en onderzoeken Datalek analyse	Monitoring toegang netwerk Evalueren proces In- en externe audits Datalek controle Pentesten
Middelen	Privacyverklaring Privacy-administratie Document management	Verklaring omtrent gedrag Geheimhoudings-verklaringen Document management	Authenticatie Autorisatie Pentesten Logging en monitoring Zorgmail Verwerkersovereenkomst

6.1. Wet- en regelgeving, normen en beleid

De toepasselijke wet- en regelgeving met betrekking tot gegevensbescherming en informatiebeveiliging is vertaald in een aantal beleidsdocumenten zoals het gegevensbeschermingsbeleid en het informatiebeveiligingsbeleid. Hierin zijn ook de eisen vanuit de landelijke normen als NEN7510 en de beroeps- en gedragscode verwerkt.

Jaarlijks wordt het beleid herzien en worden beleidsdoelstellingen geformuleerd. Hierbij wordt rekening gehouden met de in- en externe ontwikkelingen van de organisatie die van invloed zijn op de koers die gevaren wordt. Het beleid vormt kaders voor de organisatie waarbinnen persoonsgegevens volgens de wettelijke eisen worden verwerkt en waarover verantwoording kan worden afgelegd.

De betrokkenen worden geïnformeerd door middel van een privacyverklaring. In deze privacyverklaring is onder andere opgenomen van wie persoonsgegevens worden verwerkt, voor welke doeleinden, op basis van welke grondslagen, welke bewaartermijnen worden gehanteerd en welke maatregelen worden getroffen om de persoonsgegevens te beveiligen. Daarnaast worden de betrokkenen geïnformeerd over hun rechten en hoe zij deze kunnen uitoefenen en waar zij terecht kunnen met vragen, klachten of verzoeken. De verklaring is gepubliceerd op de website van Allerzorg.

In de wetgeving is opgenomen is een documentatieplicht opgenomen. Op basis daarvan heeft Allerzorg een privacy-administratie ingericht. Hierin is – naast de wettelijke registers –informatie opgenomen op basis waarvan Allerzorg kan aantonen dat aan wet- en regelgeving wordt voldaan. Centraal hierin staat het register van verwerkingsactiviteiten. Wijzigingen in de verwerkingen van

persoonsgegevens worden doorgevoerd in dit register. In 2019 is gestart met het overzetten van de huidige privacy-administratie naar een webapplicatie. In 2020 zal dit worden afgerond.

6.2. Handelen en gedrag

In 2019 is aandacht besteed aan de bewustwording van medewerkers op het gebied van gegevensbescherming en informatiebeveiliging. Door middel van nieuwsberichten op intranet en in nieuwsbrieven worden medewerkers geïnformeerd over uiteenlopende onderwerpen die met gegevensbescherming en informatiebeveiliging te maken hebben. Hierbij wordt ook ingegaan op de actualiteit. In 2020 zal regelmatig een nieuwsbericht worden geplaatst om de medewerkers blijvend bewust te houden.

In 2019 zijn een aantal nieuwe e-learningmodules van Noordhoff aan de Allerzorg Academie toegevoegd, waaronder de module 'Privacybescherming en informatieveiligheid'. Deze module is aangevuld met modules die in eigen beheer zijn ontwikkeld: gegevensbescherming en informatiebeveiliging. Deze modules zijn specifiek voor Allerzorg gemaakt. In 2020 wordt verwacht dat de medewerkers de modules gegevensbescherming en informatiebeveiliging afronden zodat zij op de hoogte zijn van wat van hen wordt verwacht in het kader van deze onderwerpen.

De gedragsregels worden in 2020 herijkt waarbij ook aandacht wordt gegeven aan het onderwerp informatiebeveiliging.

6.3. Technische en fysieke beveiliging

Authenticatie is het proces om na te gaan of iemand echt is wie hij beweert te zijn. Als basis wordt hiervoor een combinatie van een username en wachtwoord gebruikt. In 2019 is een start gemaakt om het authenticatieproces verder te verbeteren door meer-factor authenticatie af te dwingen voor toegang tot het netwerk. Hierbij wordt met naast de username/wachtwoord combinatie (de factor 'wat je weet') met een authenticator (de factor 'wat je hebt') gewerkt. In het eerste kwartaal van 2020 zal meer-factor authenticatie worden aangezet voor alle medewerkers.

Autorisatie is het proces om te waarborgen dat de gebruiker toegang heeft tot de juiste (persoons)gegevens. In 2019 is gestart met het herijken van de toegang van gegevens binnen het ECD op basis van roled based access control. Dit project wordt in 2020 afgerond. Uitgangspunt hierbij is dat medewerkers moeten beschikken over gegevens om hun werk goed, veilig en verantwoord uit te kunnen voeren.

De gebruikersactiviteiten binnen het ECD worden gelogd zodat kan worden nagegaan wie welke persoonsgegevens in het ECD heeft verwerkt. In 2020 wordt een start gemaakt met het periodiek analyseren van deze logbestanden om verantwoording af te kunnen leggen over de toegang tot de persoonsgegevens en om incidenten op te kunnen sporen.

Binnen de gezondheidszorg werken veelal zorgverleners met elkaar samen om de zorg rondom een cliënt vorm te geven. Hiervoor moeten persoonsgegevens tussen verschillende zorgaanbieders worden uitgewisseld. In veel gevallen wordt hierbij gebruik gemaakt van e-mail. Om ervoor te zorgen dat de uitwisseling van deze gegevens veilig verloopt wordt gebruik gemaakt van Zorgmail, een applicatie die de mail versleuteld aflevert bij de ontvanger. Om toegang tot het bericht te krijgen moet de ontvanger ook een gebruiker zijn van Zorgmail of krijgt een eenmalige tijdelijke code toegezonden waarmee het bericht kan worden ontsleuteld. Een groot aantal zorgverleners maakt gebruik van Zorgmail, maar nog niet iedereen. In mei 2020 zal elke zorgverlener gebruikmaken van Zorgmail.

De leveranciers van hard- en software zijn in de meeste gevallen verwerkers van persoonsgegevens. Met deze leveranciers wordt een verwerkersovereenkomst gesloten. Hiervoor wordt gebruik gemaakt van de standaard verwerkersovereenkomst zoals deze binnen de gezondheidszorg wordt gebruikt. Hiermee wordt aangehaakt bij de norm van de branche en wordt bereikt dat met één set voorwaarden afspraken worden overeengekomen met verwerkers. Dit heeft als voordeel dat een veelheid van verschillende afspraken, voorwaarden en aansprakelijkheden wordt voorkomen.

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.

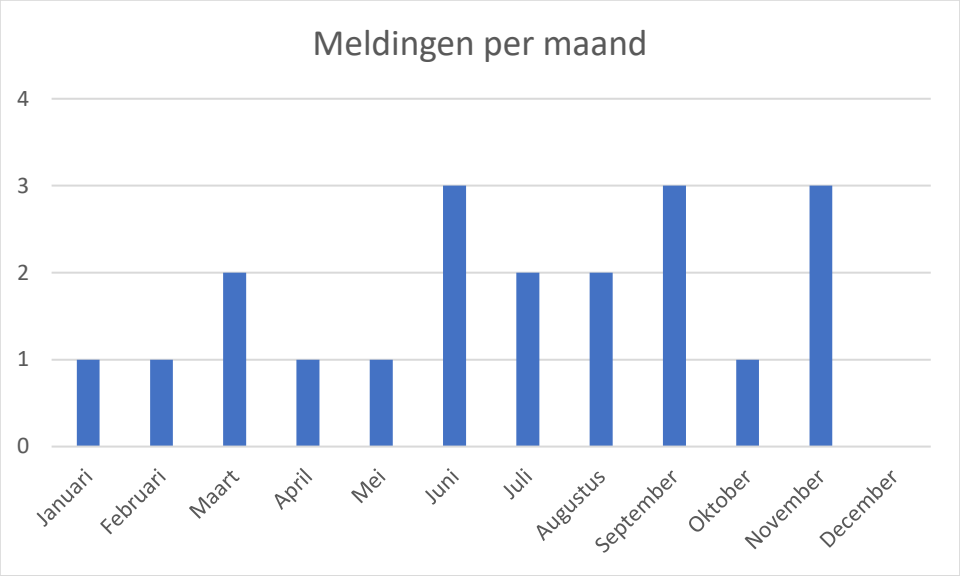
Pentesten

Er is een assessment uitgevoerd door een van onze leveranciers. Zij hebben een controle gedaan op de huidige toegangsmaatregelen tot AAD. De verbeteringen vanuit dit assessment zijn inmiddels doorgevoerd, waardoor de toegang nog verder beperkt is. In 2020 zal er een pentest worden uitgevoerd.

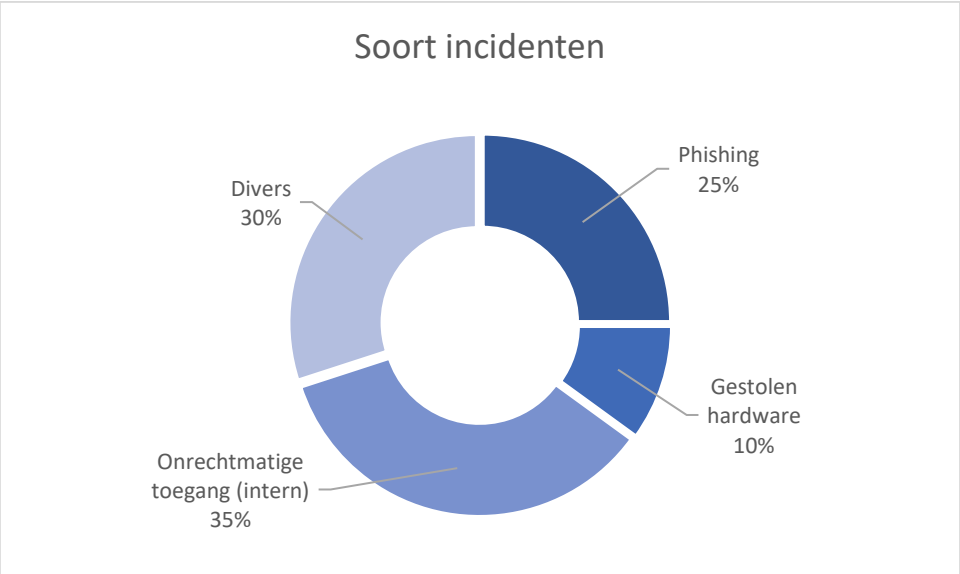
In 2019 is een onderzoek uitgevoerd naar het proces spoedaccounts. Dit proces is ontworpen om externe zorgverleners snel (buiten kantooruren) toegang te geven tot cliëntgegevens. Het betreft een geheel geautomatiseerd proces waarbij herleidbaar is wie toegang heeft tot de persoonsgegevens. Het onderzoek wijst uit dat het proces zelf een veilige en rechtmatige verwerking is. In incidentele gevallen komt het voor dat de zorgverlener ondanks het toegewezen account geen toegang tot het ECD heeft. In dat geval worden de gegevens via een beveiligde mail naar de zorgverlener verstuurd.

7. Analyse datalekken

In 2019 zijn twintig incidenten gemeld waarvan er acht een datalek bleken te zijn. Van de acht datalekken is er één aan de toezichthouder gemeld. De betrokkenen zijn eveneens over het datalek geïnformeerd. De overige zeven datalekken vormden geen risico voor betrokkenen. Wat opvalt is dat in de tweede helft van 2019 de meeste incidenten zijn gemeld, ondanks dat in december geen incident is gemeld.



De oorzaak van de incidenten is verschillend, maar het valt op dat het aantal meldingen van pogingen om gebruikers te verleiden op een 'foute' link te klikken (phishing) toeneemt. Aangenomen wordt dat dit twee oorzaken heeft: de toegenomen bewustwording van medewerkers en de toename van phishing. Hieruit blijkt dat het belangrijk is om blijvend aandacht te geven aan de bewustwording en om de phishingmails uit het berichtenverkeer te filteren.



8. Ambities voor 2020

Voor 2020 heeft Allerzorg drie ambities op het gebied van gegevensbescherming en informatiebeveiliging. De eerste ambitie is om de risico's voor betrokkenen verder minimaliseren door het uitvoeren van DPIA's[4] en het doorvoeren van technische maatregelen om de toegang tot persoonsgegevens verder te beveiligen. Dit wordt bereikt door het implementeren van een proces voor de uitvoering van DPIA's, het verscherpen van de veiligheid en rechtmatigheid van de toegang tot persoonsgegevens en het structureel beveiligen van het ad-hoc-berichtenverkeer.

De tweede ambitie is om de verantwoording over de verwerking van persoonsgegevens transparanter te maken. Hiervoor wordt een intern normenkader vastgesteld op basis waarvan het volwassenheidsniveau van (delen van) de organisatie op het gebied van gegevensbescherming en informatiebeveiliging kan worden vastgesteld en de voortgang hierin kan worden gemeten. Verder wordt verantwoording afgelegd over de gebruikersactiviteiten in het ECD door de periodieke analyse van logbestanden.

De derde ambitie heeft betrekking op het faciliteren van de rechten van betrokkenen. Om dit beter te faciliteren, wordt via een webapplicatie toegang gegeven tot hun persoonsgegevens. Hiermee heeft de betrokkene inzage in zijn dossier en kan deze gemakkelijk zijn rechten op de verwerking van zijn persoonsgegevens uitoefenen.

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

[4] Data protection impact assessment