Zonnehuisgroep Noord

Verklaring van accountability

(Verklaring van accountability2018)

Verantwoording van Zonnehuisgroep Noord aan betrokkenen over het voldoen aan wet- en regelgeving op het gebied van privacy & informatiebeveiliging.

Auteur:	Anita Meijer
Datum:	27-3-2018 vastgesteld door het MT
Versie:	1.0 definitief

Voorwoord

Informatie komt in verschillende vormen voor. Informatie kan onder meer zijn gedrukt of geschreven op papier, elektronisch zijn opgeslagen, per post of via elektronische media worden verzonden, op film worden getoond of mondeling worden uitgewisseld. Informatie behoort altijd op geschikte wijze te worden beschermd, rekening houdend met de vorm of de wijze waarop deze wordt gedeeld of opgeslagen. Voor het omgaan met informatie is een veelvoud aan wetgeving en de omvang is verder toegenomen.

In snel tempo is de wetgeving op het gebied van privacy en informatiebeveiliging aangenomen. Per 1 juli 2017 is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (gedeeltelijk) in werking getreden. Deze wet verplicht zorginstellingen om hun informatiebeveiliging conform de NEN normen in te richten. De NEN normen zijn opgesteld door de stichting Nederlands Normalisatie-instituut en specifiek gericht op de zorg:

- NEN 7510: norm voor het organisatorisch en technisch inrichten van informatiebeveiliging in de zorg;
- NEN 7512: nadere invulling van NEN 7510 betreffende de veiligheid van gegevensuitwisseling tussen partijen in de zorg;
- NEN 7513: nadere invulling van NEN 7510 betreffende het vastleggen van acties op elektronische cliëntendossiers.

Naast deze wetten is er nog een veelvoud aan wetten waar bepalingen opgenomen zijn over privacy en informatiebeveiliging. Denk hierbij onder andere aan de Wet op de geneeskundige behandelovereenkomst, de Wet langdurige zorg en de Wet kwaliteit klachten en geschillen in de zorg. Naast deze wetten is de toezichthouder, Autoriteit Persoonsgegevens (AP) gestart met het toezien op de naleving van de Europese Algemene verordening gegevensbescherming (Avg) plus de nadere uitwerking in de Uitvoeringswet (UAvg).

In deze wetgeving zijn 'Accountability' en 'Auditability' de kernbegrippen. Bescherming van de persoonsgegevens is een grondrecht en met deze gegevens moet zorgvuldig worden omgegaan door de verantwoordelijke maar ook door de verwerker of zijn subverwerker. Er is sprake van ketenaansprakelijkheid; dat wil zeggen dat de verantwoordelijke verantwoordelijk en aansprakelijk is dat ook zijn verwerkers (en mogelijke subverwerkers) de wetgeving gericht op beschermen van persoonsgegevens naleven.

Accountable zijn voor het beschermen van persoonsgegevens wil zeggen dat Zonnehuisgroep Noord de effectiviteit van de getroffen beheersmaatregelen desgewenst kan overleggen. In 2018 hebben wij ons vooral op deze wettelijke eis gericht door de privacy & security administratie op orde te brengen, de eigen organisatie en de verbonden partijen (verwerkers) in kaart te brengen en sluitende overeenkomsten mee te sluiten en stap voor stap waar het kan passende beheers- en beveiligingsmaatregelen te treffen.[1] In 2018 is een volwassenheidsniveau drie bereikt voor gegevensbescherming.

Zonnehuisgroep Noord vindt het vanzelfsprekend en van groot belang dat goed wordt omgegaan met privacygevoelige gegevens. Daarbij vindt Zonnehuisgroep Noord het belangrijk dat met de gegevens van een ander wordt omgegaan zoals iedereen zou willen dat er met de eigen persoonsgegevens wordt omgegaan.

Aan de hand van de wetgeving is en blijft Zonnehuisgroep Noord intensief aan de slag met privacy en informatiebeveiliging.

[1] Privacybescherming is voor de Zonnehuisgroep Noord belangrijk. Het betreft in eerste instantie een vraagstuk van houding en gedrag. Aan bewustzijn bij iedere medewerkers wordt permanent gewerkt. Hierbij nemen we de volgende punten mee bij het maken van keuzes:
- Privacy en gegevensbescherming mag de zorg 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;
- Zorgvuldigheid staat voorop maar het helemaal uitsluiten van datalekken is niet mogelijk.

Inleiding

1. Inleiding

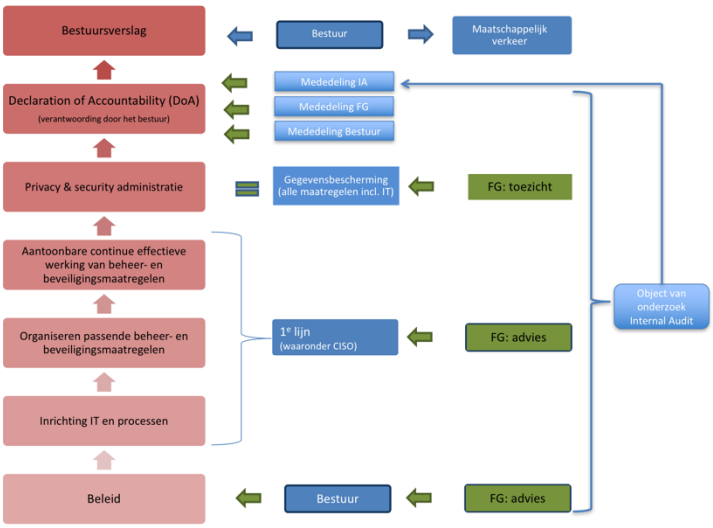
1.1. Doel Declaration of Accountability

In de Governancecode Zorg is opgenomen dat de raad van bestuur verantwoording aflegt over de realisatie van de doelstellingen van de zorgorganisatie en het gevoerde beleid ten aanzien van de belanghebbenden.
De organisatie moet transparant zijn in haar handelen en de keuzes die worden gemaakt om daar vervolgens verantwoording over af te leggen aan belanghebbenden.

In de verklaring van accountability (DoA) legt Zonnehuisgroep Noord verantwoording af aan alle belanghebbenden over de naleving van verplichtingen vanuit wetgeving op het gebied van privacy en informatiebeveiliging. Met de DoA wordt aangegeven hoe de organisatie 'in control' is en hoe de verplichtingen vanuit wetgeving worden nageleefd. Dit gebeurt op basis van al hetgeen is gedocumenteerd in de privacy & security administratie, het bewijs van effectieve werking en andere controles. Hiermee wordt een totaalbeeld van 'accountability' gegeven.

1.2. Gebruik

Privacy en informatiebeveiliging is een onderdeel van de governance (bestuur) & compliance (naleving) van Zonnehuisgroep Noord. In het onderstaand overzicht worden de stappen rondom privacy en verantwoording beschreven en welke rollen voor de verschillende personen zijn weggelegd. De Functionaris Gegevensbescherming ziet toe op het privacybeleid van Zonnehuisgroep Noord, daarbij hoort ook de toewijzing van verantwoordelijkheden, bewustmaking en opleiding en de betreffende audits. De eigenaren van applicaties en de manager bedrijfsvoering die de leiding heeft over de afdeling ICT, de Security Office Manager van Zonnehuisgroep Noord, is verantwoordelijk voor de coördinatie informatisering & automatisering. Zij zorgen voor een aantoonbare continue effectieve werking van beheer en beveiligingsmaatregelen met betrekking tot onze applicaties, het organiseren van deze maatregelen en de inrichting van de IT en processen. Uiteindelijk wordt een Verklaring van accountability(DoA) geschreven door de Functionaris Gegevensbescherming. Dit is een governance (bestuurs) verklaring en daarmee een aanvulling op de governance (bestuurs) paragraaf in het jaarlijkse bestuursverslag. De DoA is bestemd voor stakeholders (belanghebbenden) zoals cliënten, medewerkers, leveranciers, financiers en andere geïnteresseerden. De controle (op aspecten) van privacy en informatiebeveiliging is onderdeel van de controle op de jaarrekening door de accountant. De accountant kan de uitkomsten van de DoA meenemen in het vaststellen van zijn controleverklaring.



In de 'mededeling van de raad van bestuur' neemt de raad van bestuur de volledige verantwoordelijkheid op zich voor het afleggen van de verantwoording in de DoA. De raad van bestuur ondertekent de DoA. Het bestuur spreekt zich uit over het volwassenheidsniveau van gegevensbescherming en de interne auditor (André Biesheuvel RA van Duthler Associates) voert een toets uit.

2. Mededeling raad van bestuur

Wij vinden het vanzelfsprekend en van groot belang dat goed wordt omgegaan met (privacy)gevoelige gegevens. Ook vinden wij het belangrijk dat met de gegevens van een ander wordt omgegaan zoals iedereen zou willen dat er met de eigen (persoons)gegevens wordt omgegaan.

Onze cliënten, medewerkers en vrijwilligers kunnen ervan uit gaan dat wij zorgvuldig met zijn of haar gegevens omgaan. En dat begint bij bewustwording en resulteert in accountable (verantwoordelijk) zijn voor het effectief beschermen van persoonsgegeven. De verklaring van accountability hebben wij integraal onderdeel gemaakt van de jaarlijkse verantwoording aan het maatschappelijk verkeer.

De maatregelen die Zonnehuisgroep Noord in 2018 heeft genomen op het gebied van privacy & informatiebeveiliging worden in dit stuk beschreven. Hierbij laten we onze gewenste manieren niet onbesproken. We zijn trots dat wij weer een aantal belangrijke stappen vooruit hebben gezet. Wij hebben in 2018 het volwassenheidsniveau 3 bereikt en koersen in 2019 op een volwassenheidsniveau 4.

Onze ambitie voor het komende jaar hebben we verwoord in hoofdstuk 7.

Nienke Ybema 14 februari 2019

3. Mededeling Functionaris Gegevensbescherming

Zonnehuisgroep Noord is en blijft de samenhang tussen alle activiteiten op het gebied van privacy en informatiebeveiliging optimaliseren. Er wordt veel geïnvesteerd in verdere verbeteringen van het privacyvraagstuk. Binnen de organisatie hebben we in 2018 samen een mooie stap gemaakt in het kader van privacy en informatiebeveiliging 'van inzicht en plan van aanpak naar overzicht en inzicht'.

Er zijn geen vragen van betrokkenen geweest om hun rechten uit te oefenen. Dat wil niet zeggen dat deze vragen er niet zijn. Het proces van gedragsverandering voor cliënten en medewerkers is gaande. Op dit moment zijn de rechten van betrokkenen voldoende ingeregeld. De gespecificeerde toestemming waaraan we moeten voldoen in 2020 roept nog de nodige vragen op.[2]

We werken in een keten en het is af en toe lastig de partners in het netwerk te overtuigen van de wettelijke plicht van het afsluiten van een verwerkersovereenkomst of een gegevenswisselingsovereenkomst, afspraken te maken over privacy en informatiebeveiliging. Dit is bestuursrechtelijk geregeld. Belangen zijn tegenstrijdig om eraan te voldoen, kennisniveau is soms te laag. Kwaliteit met samenwerkingspartijen vraagt aandacht.

Wat hebben we in 2018 gerealiseerd:

- Een privacy- & security administratie is aangeschaft en ingericht;
  In deze administratie worden de verwerkingen en getroffen beheers- en beveiligingsmaatregelen vastgelegd en ook de uitkomsten van effectieve werking van door Zonnehuisgroep Noord en haar partners getroffen beheers- en beveiligingsmaatregelen,
  register van verwerkingen;
- Werkgroep Privacy & Informatiebeveiliging (WP&I) ingericht en fungeert ook als crisisteam voor de afhandeling van grote datalekken;
- Breed toepassen van smart contracting verwerkersovereenkomst met als doel de ketenaansprakelijkheid beheersbaar te krijgen en te houden;
- Meldprocedure datalekken;
- Procedure Privacy Impact Assessment (PIA), bij het contracteren van nieuwe partijen wordt er een PIA uitgevoerd en van alle kernapplicaties is een PIA uitgevoerd;
- Opstellen en actualiseren van het privacy- en Informatiebeveiligingsbeleid, privacyverklaring, gedragscode en regels, privacyreglement medewerkers;
- De rechten van betrokkene ingeregeld;
- Start gemaakt met het bewustwordingstraject door middel van 2 maandelijkse nieuwsbrieven en een presentatie door de managers gegeven over privacy & informatiebeveiliging aan medewerkers;
- Verdiepingsslag gemaakt voor de aanschaf van een bewustwording programma die aansluit bij alle medewerkers van Zonnehuisgroep Noord;
- Verdiepingsslag gemaakt met de toepassing van het NFU normenkader in de organisatie en systemen van Zonnehuisgroep Noord;
- Technische security maatregelen zijn geoptimaliseerd;
- Verdiepingsslag gemaakt met betrekking tot het beter vastleggen van de besluitvorming over updates van systemen en het testen hiervan, afgesproken vernietigingstermijnen worden gehanteerd in de systemen en in de organisatie, applicatie logboek is ontwikkeld waarin alle belangrijke mutaties rondom applicaties zijn opgenomen.

Regelmatig heb ik overleg met de Werkgroep Privacy & Informatiebeveiliging (WP&I) en de leiding van Zonnehuisgroep Noord over de voortgang van de getroffen beheersmaatregelen.
De ambitieuze doelstelling voor 2018 was om volwassenheidsniveau 3-4 voor het einde van het jaar te bereiken. Volwassenheidsniveau 3 is bereikt voor 2018.

In deze DoA worden alle in 2018 ondernomen acties verantwoord.
Ook worden eventuele verbeterpunten en de ambitie voor de komende periode benoemd.
Met de door de leiding gekozen governance (bestuur) en compliance (naleving) structuur geeft mij als Functionaris Gegevensbescherming een stevige basis mijn functie uit te oefenen.

In 2019 zal Zonnehuisgroep Noord doortastend moeten handelen om een volwassenheidsniveau

[2] Zie hiervoor het rapport van de ombudsman:
https://www.nationaleombudsman.nl/onderzoeken/2018085-van-wie-die-privacy-eigenlijk-uitgangspunten-voor-samenwerkende-professionals
en van de patiëntenvereniging:
https://www.patientenfederatie.nl/images/stories/dossier/patientgeheim/RapportPrivacyindezorg.pdf .

4-5 aan het eind van 2019 te halen. Met de getroffen voorbereidingen in 2018 zal de WP&I goed kunnen sturen om de uitvoer in 2019 te realiseren. Een opsomming:

- Permanente bewustwordingsprogramma voor sleutelmedewerkers en medewerkers. De FG volgt de voortgang van de medewerkers en ondersteunt de medewerkers waar nodig. Het bewijs van de effectiviteit van het programma wordt vastgelegd in de privacy & informatieveiligheidadministratie;
- Structurele toepassing van het NFU normenkader in de organisatie en systemen van Zonnehuisgroep Noord. Ook zijn de eisen rondom gegevensbescherming en het NFU normenkader opgenomen in het compliance control framework (kader naleving);
- Met verwerkers afspreken en de noodzaak bespreken, dat zij eveneens een privacy & security boekhouding voeren waardoor zij ook aantoonbaar auditable (controleerbaar) zijn;
- Op het merendeel van de applicaties een Privacy Impact Asssessment (PIA) uitvoeren;
- Structurele toepassing met betrekking tot het beter vastleggen van de besluitvorming over updates van systemen en het testen hiervan, afgesproken vernietigingstermijnen worden gehanteerd in de systemen en in de organisatie, applicatie logboek is ontwikkeld waarin alle belangrijke mutaties rondom applicaties zijn opgenomen. Bespreken van de logging om de risico impact in te beoordelen.
- Ter voorbereiding op de gespecificeerde toestemming van betrokkenen hiervoor het fundament faciliteren. De voorbereiding treffen van een bedrijfsspecifieke data gedreven omgeving naar een omgeving waar de betrokkene 'in control' is;
- Regelmatig in overleg treden met de Werkgroep Privacy & Informatiebeveiliging en de leiding van Zonnehuisgroep Noord over de voortgang van getroffen beheersmaatregelen.

De FG zoekt het gesprek in de organisatie op.

Begin 2018 heb ik het Regionaal Netwerk FG in het noorden opgezet en ook binnen de leergang Functionaris Gegevensbescherming zijn mogelijkheden de samenwerking op te zoeken met instellingen die voor dezelfde taak staan.

Sinds september 2017 volg ik de leergang FG bij Duthler. Mijn studieresultaten zijn positief en ik verwacht de studie in november 2019 af te ronden.

In 2018 ben ik vanuit Zonnehuisgroep Noord gedetacheerd bij De Hoven en Hoogwatum in de functie FG.

In mijn werkzaamheden en taken van Functionaris Gegevensbescherming zal ik zoveel mogelijk ervaringen uitwisselen en modellen die Zonnehuisgroep Noord passen toepassen.

Anita Meijer 14 februari 2019
Functionaris voor Gegevensbescherming

4. Mededeling interne auditor

De interne controle naar de getrouwheid van de mededeling door de raad van bestuur (rvb) alsmede de rapportage van de functionaris voor gegevensbescherming (FG) van de Zonnehuisgroep Noord over 2018 en weergegeven in dit document, de 'Verklaring van Accountability 2017' (Declaration of Accountability (DoA), is verzorgd door Duthler Associates, drs. A.J. Biesheuvel RFG RE RA.[3],[4]

Zonnehuisgroep Noord verwerkt persoonsgegevens van haar cliënten, van sollicitanten en medewerkers (eigen en ingehuurd) en van vrijwilligers. De persoonsgegevens die van cliënten worden bijgehouden worden omschreven als kritische persoonsgegevens, veelal medische van aard. Zonnehuisgroep Noord heeft bij monde van de rvb in 2018 actief beleid ingezet om de organisatie naar een niveau van gegevensbescherming te brengen opdat Zonnehuisgroep Noord medio 2018 aan de Europese Algemene verordening gegevensbescherming (Avg) en de uitvoeringswet kan voldoen. De Avg is niet de enige wetgeving waaraan de Zonnehuisgroep Noord wenst te voldoen. In het legal policy framework wordt ook rekening gehouden met nieuwe sectorale wetgeving zoals de 'Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg'. Deze wijzigingen hebben invloed op het beleid van Zonnehuisgroep Noord.

Scope van de Internal Audit

De raad van bestuur heeft in nauw overleg met de functionaris gegevensbescherming besloten het beleid in stappen te implementeren. Daartoe volgt Zonnehuisgroep Noord het ambitieplan van MYOBI (https://www.myobi.eu) waarin niveaus van volwassenheid zijn opgenomen.

Duthler Associates heeft een intern onderzoek, een Internal Audit, ingesteld naar de juistheid en volledigheid van de bereikte doelstellingen voor 2018 vanuit het beleid en welke zijn verantwoord in de DoA 2018. De scope van het onderzoek is daarbij beperkt tot het vaststellen van de feiten zoals deze zijn vermeld in de hoofdstukken 2 tot en met 6 van de DoA.

Voor het uitvoeren van deze interne audit is een auditplan opgesteld en uitgevoerd. Het auditplan is met de FG gedeeld.

Uitkomsten van het Internal Audit onderzoek

Op basis van de uitkomsten van het onderzoek is gebleken dat de Zonnehuisgroep Noord de doelstelling om het ingestelde beleid om tot en met volwassenheidsniveau "drie" te komen, heeft uitgevoerd.

Aanbevelingen naar aanleiding van het onderzoek

De Zonnehuisgroep Noord heeft een IT sourcing strategie 2018 opgesteld, heeft voorbereidingen getroffen in 2018 en gaat de strategie in 2019 daadwerkelijk implementeren. Het realiseren van de IT strategie raakt de governance & compliance van de Zonnehuisgroep Noord.

De governance en compliance van gegevensbescherming wordt ook geraakt door het van kracht worden van nieuwe wet- en regelgeving en nadere uitleg van bestaande wetgeving door de toezichthouders. Beide ontwikkelingen vragen om een revisie van het legal policy framework en baseline alsmede het beleid 2019. Het in 2019 streven naar een volwassenheidsniveau vier is realistisch.

Het implementeren en vervolgens in beheer nemen van de IT sourcing (eerst 1:1 over en vervolgens doorvoeren van optimalisatieslagen) vraagt om een volledige inzet van de FG over 2019 en eventueel daarna. Aandachtsgebieden voor de agenda voor de FG:

---

[3] Ingeschreven in het FG register van Duthler Associates (https://www.duthleracademy.nl/functionaris-voor-gegevensbescherming-register/?token=ZGFjMDMw)

[4] Zie Opdrachtbevestiging Zonnehuisgroep Noord inzake Internal Audit gericht op het afgeven van een Mededeling Internal Audit bij de Declaration of Accountability betreffende het beschermen van persoonsgegevens, d.d. 18 december 2018.

1. Organiseren en plannen van het toetsen, vaststellen en vastleggen dat de verwerkers van persoonsgegevens de waarborg van effectieve werking beheersmaatregelen gericht op beschermen persoonsgegevens nakomen;
2. Het beschermen van persoonsgegevens is in eerste instantie een vraagstuk van gewenst gedrag. Doorvoeren van trainen van sleutelfunctionarissen en doorvoeren van het bewustwordingsprogramma medewerkers in 2019 waarbij de effectieve werking van het programma wordt vastgelegd. Het gevolg zal zijn dat er meer datalekken worden gemeld en deze kunnen worden gebruikt voor het delen van leermomenten; en
3. Aandacht voor het verkrijgen van bewijs van effectieve werking beheersmaatregelen en deze informatie opnemen in een proces van monitoren.

Vergeleken met andere instellingen pakt Zonnehuisgroep Noord de informatie hygiëne professioneel op. Dit leidt niet alleen tot het adequaat beschermen van persoonsgegevens maar moet ook kunnen leiden tot een effectievere en kostenefficiënter informatiehuishouding.

In het kader van het bereiken van volwassenheidsniveau vier voor eind 2019 adviseren wij u in november 2019 wederom een Internal Audit onderzoek uit te laten voeren om zekerheid te krijgen dat na de implementatie van de IT sourcing Zonnehuisgroep Noord accountable blijft en de verwachte resultaten worden geboekt.

Drs. A.J. Biesheuvel RFG RE RA

8 februari 2019

5. Vastleggen persoonsgegevens

Zonnehuisgroep Noord legt persoonsgegevens vast van haar cliënten, medewerkers en vrijwilligers. Inherent aan het werk van Zonnehuisgroep Noord legt zij veel privacygevoelige gegevens vast. Een groot deel van de verwerkingen betreffen zogenaamde bijzondere gegevens, te weten gegevens betreffende de gezondheid. Bijkomende bijzonderheid is dat de cliënten zich veelal in een kwetsbare levensfase bevinden en in de begeleiding ook ketenpartners en naastbetrokkenen een belangrijke rol spelen. De verwerkingen van persoonsgegevens zijn door Zonnehuisgroep Noord vastgelegd in het verwerkingsregister van de privacy & security administratie.

Zonnehuisgroep Noord heeft haar verwerkingen vastgelegd in de privacy & security administratie. Hierbij worden de volgende gegevens opgenomen:

- Omschrijving van de verwerking en de rechtmatigheid grondslag om deze te mogen verwerken;
- Met welk doel de persoonsgegevens worden verwerkt;
- Welke partijen er betrokken zijn bij het verwerken van de persoonsgegevens;
- Welke gegevens er vastgelegd worden;
- Welke maatregelen Zonnehuisgroep Noord heeft genomen ten aanzien van de beveiliging van de persoonsgegevens;
- Welke processen en systemen er betrokken zijn bij de verwerking;
- Op welke wijze de betrokkene toestemming heeft gegeven voor het verwerken van de Persoonsgegevens.

Naast de gegevens van cliënten en medewerkers administreert Zonnehuisgroep Noord ook gegevens van sollicitanten, raad van toezicht, cursisten, vrijwilligers, familie en naasten van cliënten, contractpartners, uitzendkrachten, ZZP'ers, detachanten en ketenpartners. Van al deze verwerkingen van (persoons)gegevens zijn gedeeltelijk en alle doelen en de specifieke gegevens die verwerkt worden zijn vastgelegd in de privacy & security administratie.

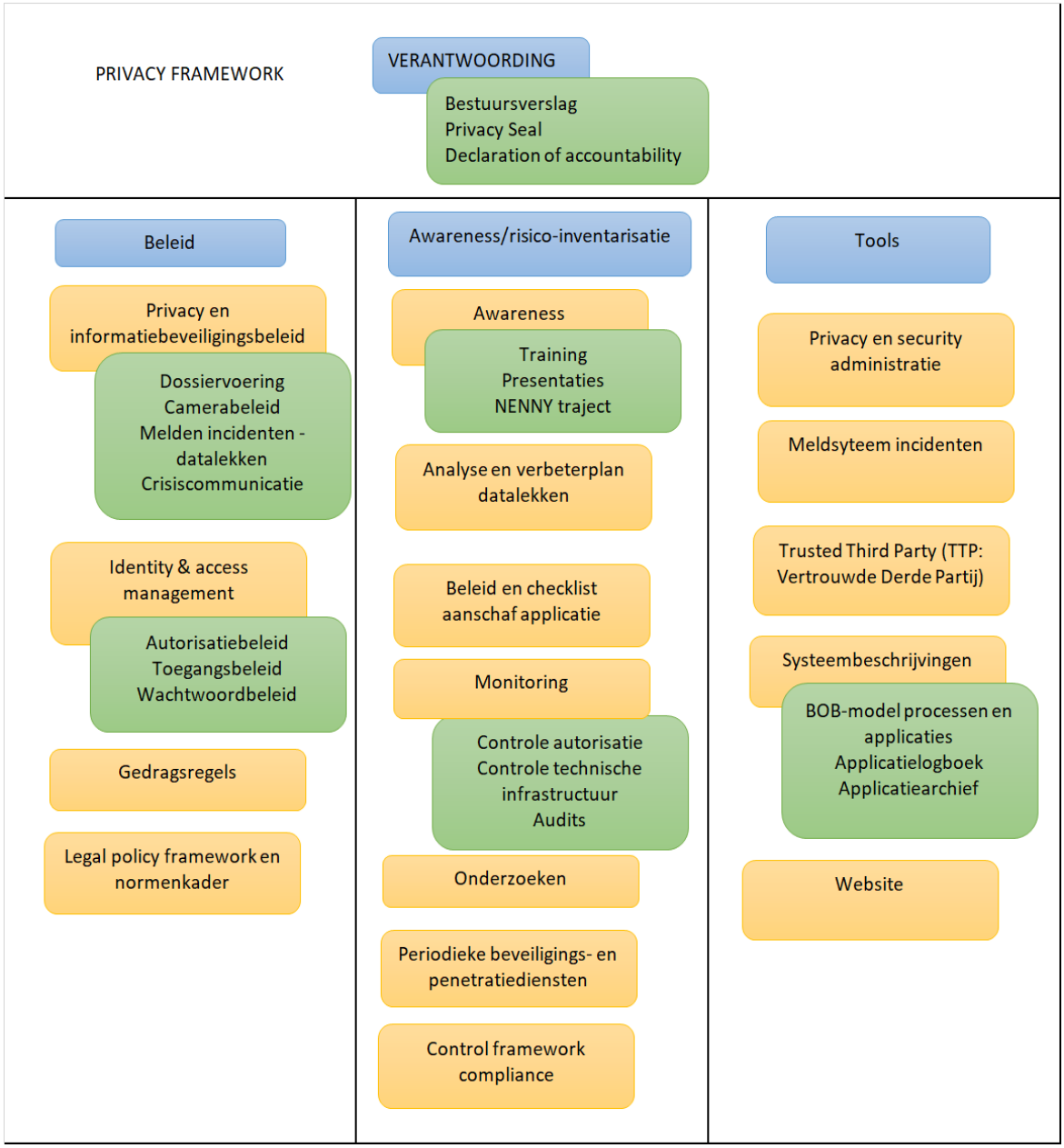
Een verwerkersovereenkomst is een overeenkomst tussen verantwoordelijke voor de persoonsgegevens en de verwerker, hierin wordt vastgelegd hoe de verwerker met de persoonsgegevens moet omgaan. De verwerker is degene die persoonsgegevens verwerkt in opdracht van de verantwoordelijke. De Avg benoemt een aantal specifieke punten die opgenomen dienen te worden in deze overeenkomst.

Zonnehuisgroep Noord sluit met alle verwerkers een verwerkersovereenkomst. Medewerkers van Zonnehuisgroep Noord en andere zorgverleners die door Zonnehuisgroep Noord worden ingehuurd hebben geheimhoudingsplicht die geldt voor alle persoonsgegevens die Zonnehuisgroep Noord verwerkt.

6. Privacy framework (privacy kader)

Het privacy framework is een overzicht van onze privacy en informatiebeveiligingshuishouding. In dit framework wordt onderscheid gemaakt tussen beleid, bewustwording / risico inventarisatie en de tools die Zonnehuisgroep Noord hiervoor inzet. Onder het framework zijn de beleidsmatige aspecten verder toegelicht. Het privacy en informatiebeveiligingsbeleid valt uiteen in een intern en een extern privacybeleid.

Zonnehuisgroep Noord zal aan de hand hiervan beschrijven wat de stand van zaken is, waar verbeterpunten liggen en welke ambitie Zonnehuisgroep Noord heeft voor de komende periode.



6.1. Verantwoording

De verantwoording over de stand van zaken op het gebied van privacy & informatiebeveiliging aan alle betrokkenen en toezichthouders doet Zonnehuisgroep Noord op verschillende manieren. In de DoA verantwoordt Zonnehuisgroep Noord zich uitvoerig over het gevoerde beleid en de ambitie voor de komende periode ten aanzien van de bescherming van persoonsgegevens. Een samenvatting van de DoA wordt opgenomen in het bestuursverslag.

Zonnehuisgroep Noord is aangesloten bij Myobi. Myobi is een onafhankelijke derde partij die een privacy keurmerk heeft verstrekt aan Zonnehuisgroep Noord. Met dit privacy keurmerk geeft Zonnehuisgroep Noord op de website van Myobi en op de eigen website het volwassenheidsniveau aan van de naleving van de privacywetgeving.

6.2. Beleid

Het beleid van Zonnehuisgroep Noord is verwoord in verschillende documenten waar een samenhang tussen bestaat. Hieronder is per document het doel en de voortgang omschreven.

Privacy & informatiebeveiligingsbeleid

In mei 2018 is het intern privacy & informatiebeveiligingsbeleid van Zonnehuisgroep Noord geactualiseerd. Dit beleid geeft richting aan de invulling van het privacyreglement en de visie en uitgangspunten die Zonnehuisgroep Noord hanteert met betrekking tot privacy en informatiebeveiliging vraagstukken. Het doel van het privacybeleid is om de kaders te stellen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens die voldoet aan de wettelijke eisen. Naast het interne privacybeleid is in september 2018 de privacyverklaring gerealiseerd en op de website van Zonnehuisgroep Noord geplaatst. In de privacyverklaring wordt aangegeven hoe Zonnehuisgroep Noord omgaat met persoonsgegevens van externen zoals cliënten en bezoekers op de website. De rechten van betrokkenen met betrekking tot de verwerking van de persoonsgegevens is hierin opgenomen.

Privacyreglement Medewerkers, vrijwilligers en sollicitanten

Zonnehuisgroep Noord heeft ter bescherming van de privacy van haar medewerkers, vrijwilligers en sollicitanten een privacyreglement. De rechten van betrokkenen met betrekking tot de registratie van de persoonsgegevens is hierin opgenomen.
In de arbeidsovereenkomst en vrijwilliger overeenkomst wordt verwezen naar het privacyreglement. Om de bestaande medewerkers te voorzien van de informatie wordt gebruik gemaakt van de website van Zonnehuisgroep Noord https://www.zonnehuisgroepnoord.nl/informatiebeveiliging-en-privacy , intranet, IDocument en het medewerkerportaal. Vrijwilligers ontvangen Q1 2019 het privacyreglement van hun vrijwilliger coördinatoren.

Gedragscode en gedragsregels

Zonnehuisgroep Noord heeft in mei 2018 gedragscode en gedragsregels informatiebeveiliging & privacy vastgesteld. Het is belangrijk dat er zorgvuldig met informatie van Zonnehuisgroep Noord omgegaan wordt, daarom gelden bij Zonnehuisgroep Noord informatiebeveiligings- en privacyregels. In de arbeidsovereenkomst en vrijwilliger overeenkomst wordt verwezen naar de gedragscode en gedragsregels. Om de bestaande medewerkers te voorzien van de informatie wordt gebruik gemaakt van intranet, IDocument en het medewerkerportaal. Vrijwilligers ontvangen Q1 2019 de gedragscode en gedragsregels van de vrijwilliger coördinatoren.

Autorisatie en authenticatie beleid

In 2018 heeft Zonnehuisgroep Noord zich gericht op de voorbereiding van een transparant en vastgesteld autorisatiebeleid en daarnaast periodieke controles van de autorisaties op alle (kern)systemen. Het autorisatiebeleid geeft aan wie waarvoor toegang heeft in een bepaalde applicatie en welke periodieke controle daarop plaatsvindt. Om het proces van het beheren van autorisaties beter te kunnen managen worden de volgende procedures in 2019 herzien en aangescherpt:

- proces in- door- en uitstroom
- aanvraag account
- proces aanvraag autorisatie externen

Authenticatie is het proces waarbij nagegaan wordt of iemand echt is wie hij beweert te zijn. Voor het inloggen van de Citrix omgeving wordt gebruik gemaakt van gebruikersnaam en een sterk wachtwoord wat periodiek gewijzigd moet worden. Als medewerkers buiten de kantooromgeving Citrix willen benaderen is een token nodig (two way authenticatie) dat wordt

gegenereerd door een fysiek apparaat dat in het bezit dient te zijn van de betreffende gebruiker.

In 2019 wil Zonnehuisgroep Noord gaan werken met single-sign-on (SSO), dit stelt eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk op het gebruikte apparaat gedurende een bepaalde periode. Het beheer van de administratie van gebruikers wordt belegd bij een externe partij onder regie van de manager bedrijfsvoering van Zonnehuisgroep Noord.

Legal policy framework / Normenkader
Vanuit de RIBW Alliantie heeft Duthler Associates eind 2016 een legal policy framework en normenkader gemaakt. In dit legal policy framework is alle relevante wetgeving op het gebied van privacy en gegevensbescherming in kaart gebracht. Dit normenkader is gebruikt voor het opstellen van bewaartermijnen. Rekening houdend met specifieke wetgeving en eventuele conflicten tussen deze wetgeving. Zo worden er bijvoorbeeld in verschillende wetten andere eisen gesteld ten aanzien van bewaartermijnen. In 2019 wordt door de organisatie een verdiepingsslag gemaakt om de handhaving op de vernietigingstermijnen van gegevens te optimaliseren.

6.3. Bewustwording / risico inventarisatie verder uitwerken adhv privacy framework

6.3.1. Bewustwording

Zonnehuisgroep Noord besteedt aandacht aan de bewustwording van medewerkers op het onderwerp privacy & informatiebeveiliging. In september 2017 is de Functionaris Gegevensbescherming gestart met de leergang (30 modules) voor Functionaris Gegevensbescherming. Ze heeft tot januari 2019, 22 modules gevolgd en de bijbehorende tentamens afgerond. Deze scholing gaat verder in 2019 en de verwachting is dat de opleiding in november 2019 volledig wordt afgerond.

In 2018 is er op meerdere momenten aandacht besteedt aan het onder de aandacht brengen van privacy en informatiebeveiliging. Er zijn presentaties gegeven in het management- coaches en adviseurs overleg. De teamrol ICT voor sleutelfiguren binnen de teams is in ontwikkeling met onder andere aandachtsgebied privacy & informatiebeveiliging. Deze sleutelfiguren gaan de kennisoverdracht binnen de teams verzorgen en bewaken, zodat dit onderwerp een terugkerend agendapunt tijdens werkoverleggen wordt. Specifiek promotiemateriaal wordt ontwikkeld en er is een informatiebeveiliging & privacy checklist voor medewerkers en vrijwilligers opgesteld. Verder staat er informatie op IDocument en intranet, zoals een maandelijkse nieuwsbrief, veelgestelde vragen (FAQ) en checklist. In de Bewustwording wordt ook aandacht besteed aan het laagdrempelig melden van eventuele datalekken.
De procedure datalekken is in oktober 2018 vereenvoudigd en geactualiseerd.

In 2019 wil Zonnehuisgroep Noord de bewustwording van medewerkers verder vergroten. Hiervoor zijn in 2018 diverse e-learning mogelijkheden onderzocht.
Hieronder is een overzicht opgenomen van de bewustwording initiatieven in de periode 1 januari 2018 tot november 2018:

- Scholing FG — continue
- Privacy en informatiebeveiliging op de agenda van het MT — 6x
- Werkgroep Privacy & Informatiebeveiliging (WP&I) — 1x per 6 weken
- Presentatie privacy en informatiebeveiliging managers, coaches en medewerkers — 1x
- NENny nieuwsbrief organisatiebreed — 2 maandelijks

Onderdeel van de bewustwording is ook het informeren van betrokkenen over hun rechten. Medewerkers, vrijwilligers en cliënten zijn geïnformeerd over hun rechten in de privacyverklaring op de website. Voor cliënten Zonnehuis Thuis is het cliënten-/mantelzorgers portaal ONS Nedap CarenZorg in 2017 opengesteld. Door middel van dit portaal hebben cliënten en mantelzorgers toegang tot (delen van) het dossier. In 2018 is de start gemaakt dat ook de intramurale cliënten het cliënten-/mantelzorgers portaal QIC toegankelijk wordt. Voor 2019 is de doelstelling om de rechten van alle betrokkenen zo volledig mogelijk te faciliteren.

6.3.2. Privacy Impact Analyse (PIA) "gegevenseffectbeoordeling"

De Privacy Impact Analyse geeft inzicht in welke risico's er zijn met betrekking tot de verwerking van persoonsgegevens zodat er vooraf maatregelen genomen kunnen worden om deze risico's te beperken.

Procedure Privacy Impact Assessment (PIA), bij het contracteren van nieuwe partijen wordt er een PIA uitgevoerd en van alle kernapplicaties is in 2018 een PIA uitgevoerd.

6.3.3. Analyse van datalekken

Datalekken zijn onderzocht door de functionaris Gegevensbescherming. Zonnehuisgroep Noord heeft een open cultuur waarin datalekken laagdrempelig gemeld worden. Het onderzoek van de datalekken is er primair op gericht om ervan te leren. Voor het onderzoek wordt gebruik gemaakt van de procedure melding datalekken. Op basis van het onderzoek geeft de Functionaris Gegevensbescherming een advies aan de Security Office Manager en het bestuur. In 2018 is er niet afgeweken van het advies van de Functionaris Gegevensbescherming. Het bestuur beslist of een datalek gemeld wordt bij de Autoriteit Persoonsgegevens en/of de betrokkenen. Bij de Functionaris Gegevensbescherming zijn in 2018 in totaal 26 datalekken gemeld. Dit waren 21 incidenten en 5 datalekken. Er is door 1 leverancier (verwerker) een datalek gemeld. De datalekken zijn gemeld bij de Autoriteit Persoonsgegevens. Bij een ernstig datalek moet Zonnehuisgroep Noord het datalek ook aan de Autoriteit Persoonsgegevens melden. 4 datalekken zijn gemeld aan betrokkenen. 1 datalek is niet gemeld aan de betrokkenen, omdat we er redelijkerwijs vanuit kunnen gaan, dat er geen kans is op gevolgen voor de persoonlijke levenssfeer van de betrokkenen.

De Algemene Verordening Gegevensbescherming (Avg) verplicht om bij datalekken snel onderzoek te doen en in het geval van ernstige inbreuk op de privacy dit binnen 72 uur te melden aan de Autoriteit Persoonsgegevens en/of de betrokkenen.
Het is in 2018 gelukt het onderzoek binnen de 72 uur te doen. De verwachting is, dat Zonnehuisgroep Noord ook in 2019 binnen 72 uur kan blijven melden bij de Autoriteit Persoonsgegevens.

6.3.4. Onderzoeken

In 2018 vond er één onderzoek plaats. Dit onderzoek was preventief en gericht op de infrastructuur IT. Er deed zich geen specifieke bedreiging voor. Naar aanleiding van de uitkomsten in maart 2018 van het technische security beveiliging onderzoek heeft Zonnehuisgroep Noord zich laten informeren hoe de technische security maatregelen verbeterd kunnen worden. Hiervoor is een plan van aanpak gemaakt welke in 2018 en 2019 uitgevoerd wordt. Daarnaast is in 2018 de uitvoer Privacy Impact Analyse op de kernapplicaties gerealiseerd en bij aanschaf nieuwe applicaties. De Privacy Impact Assessments worden in 2019 en verder uitgevoerd voor alle persoonsgegevensstromen inclusief bijbehorende applicaties.

6.3.5. Checklist aanschaf applicatie

Medio 2018 heeft Zonnehuisgroep Noord bij de aanschaf van een nieuwe applicatie een checklist om de risico's op privacy, informatiebeveiliging en voor privacy by design gebruikt om ervoor te zorgen, dat er geen zaken over het hoofd worden gezien. En de applicatie voldoet aan wet- en regelgeving. De checklist is opgenomen in het invuldocument Privacy Impact Assessment (PIA).

6.3.6. Periodieke beveiligings- en penetratietesten

Technische security maatregelen zal Zonnehuisgroep Noord in 2019 verder onderzoeken en indien nodig actie ondernemen om applicaties en/of infrastructuur op beveiligingsissues en kwetsbaarheden. Jaarlijks kan op basis van een risico inschatting eventueel worden gekeken welke applicatie en/of infrastructuur onderzocht gaat worden. Het onderzoek kan ook gericht zijn op gedrag of toetsing van procedures. Ook penetratietesten kunnen in de toekomst worden uitgevoerd. Eventuele onderzoeksresultaten worden opgenomen in de privacy- en security boekhouding.

6.3.7. Monitoring

Om goed invulling te geven aan het begrip accountability in de Algemene Verordening Gegevensbescherming heeft Zonnehuisgroep Noord in 2018 in kaart gebracht wat wenselijk is en wordt in 2019 zaken geïmplementeerd als:

Controle autorisaties
Periodieke controles uitgevoerd door de functioneel beheerders van de applicaties. Hierbij wordt gecontroleerd of de gebruikers in het systeem enerzijds nog een relatie hebben met Zonnehuisgroep Noord en anderzijds of hun rol nog past bij de rechten waarover zij binnen de applicaties beschikken. Niet alleen vanuit functioneel perspectief, maar ook vooral met het oog op privacy- en informatiebeveiliging is het van groot belang dat de autorisaties up to date zijn. Uitgevoerde controles moeten worden gerapporteerd en controlelijsten, resultaten van opschoningen worden opgeslagen ter archivering. Er zal een functioneel beheerdersoverleg plaatsvinden waar de daadwerkelijke uitvoering van de controles wordt gemonitord.

Continue monitoring (technische infrastructuur)
Vanuit het onderzoek beschreven in 6.3.4. technische security maatregelen zal Zonnehuisgroep Noord in 2019 optimaliseren hoe we eventueel (nog beter) gebruik kunnen maken van tooling waarmee de kwetsbaarheden van het interne netwerk en alle actieve netwerkapparatuur worden gemonitord. De mogelijkheid voor systeembeheerders om de bevindingen te rapporteren in een dashboard voor systeembeheerders. Ook wordt hierin meegenomen om een aantal websites en toegangsportalen van Zonnehuisgroep Noord middels tooling continu te monitoren op kwetsbaarheden. De te toetsen onderdelen, bedreigingen en mogelijke kwetsbaarheden moeten constant up-to-date worden bijgehouden en volgen de laatste trends en ontwikkelingen. Het proces van bewaking en controle van deze tooling, alsmede de opvolging voor het verhelpen van kwetsbaarheden moet worden vastgelegd als onderdeel van de systeembeschrijvingen. Dit proces moet worden belegd bij systeembeheer.
Bevindingen moeten worden geprioriteerd en voor opvolging als meldingen worden opgenomen in eventuele helpdesk software.

6.3.8. Control Framework

Per 1 juli 2017 is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (gedeeltelijk) in werking getreden. Deze wet verplicht zorginstellingen om de informatiebeveiliging conform de NEN normen in te richten. Zonnehuisgroep Noord zal in 2018 en 2019 informatiebeveiliging opnemen in het compliance (naleving) control framework. Vanuit dit framework zal doorlopend risico's in kaart gebracht worden en periodiek audits en of verbeteracties gepland. In 2018 zijn de processen en sub processen informatiestromen van persoonsgegevens in kaart gebracht. In 2019 wordt dit verder uitgewerkt met de risico’s die hieruit kunnen voortvloeien.

6.4. Tools

In 2018 heeft Zonnehuisgroep Noord stevig geïnvesteerd in tools, vanwege de complexiteit van privacy & informatiebeveiliging en doordat privacy en informatiebeveiliging in alle onderdelen van de organisatie terugkomt.

Privacy & security administratie
Het hart van alle activiteiten rondom privacy en informatiebeveiliging is de privacy- en security administratie (PSA). In 2018 heeft Zonnehuisgroep Noord hiervoor software aanschaft: het SBC managementsysteem. In deze software wordt vanaf januari 2018 de volgende zaken vastgelegd:

- Overzicht met de verbonden partijen waarmee Zonnehuisgroep Noord persoonsgegevens uitwisselt;
- Omschrijving van alle verwerkingen met doelen, stakeholders, gegevenssets, maatregelen, processen en informatiesystemen;
- Verantwoording van alle door Zonnehuisgroep Noord gedane activiteiten op het gebied van privacy & informatiebeveiliging;
- Onderzoeken die door Zonnehuisgroep Noord gedaan zijn;
- Onderzoek van datalekken.

In 2019 wil Zonnehuisgroep Noord deze administratie verder optimaliseren en aanvullen met:

- controle op de volledigheid van alle in gebruik zijnde systemen;
- controle op de volledigheid van de verbonden partijen;
- toevoeging van het Legal Policy Framework en het normenkader;
- koppelen van verwerkingen aan eigenaren en functioneel beheerders.

Het verwerkingen register is geen eenmalige registratie, maar een organisch proces. Het registreren moet daarom op structurele wijze opgenomen worden in de organisatie. Naast nieuwe verwerkingen dient het register aangevuld te worden met de technische routering-, transport- en beveiligingsmaatregelen of -componenten die ook verwerkingen betreffen en dienen de processen en systemen daarvan op de juiste wijze hieraan gekoppeld te worden. Het onderhoud van het systeem moet onderzocht worden hoe we dit de komende jaren kunnen borgen. Een gedachte is dit over te dragen aan de functioneel applicatiebeheerders en de eigenaren van de applicaties.

Meldsysteem incidenten

Het melden van incidenten is in de eerste plaats bedoeld om te leren. De inhoudelijke lessen, maar zeker ook het proces van het melden, leiden tot een verbetering van de veiligheid en kwaliteit van een organisatie. Een melding is het startsein voor feedback en dus het proces van verbetering. Zonnehuisgroep Noord kiest er op dit moment voor, dat datalekken en incidenten rechtstreeks gemeld worden aan de Functionaris Gegevensbescherming, zodat de melding direct onderzocht wordt. Op een later moment kan worden besloten de meldingen eventueel via een meldsysteem te laten lopen.

Applicatie beschrijvingen / applicatie logboek en documentenbeheer

Binnen Zonnehuisgroep Noord is veel informatie over alle applicaties beschikbaar, maar niet op een gestructureerde manier. In 2018 heeft Zonnehuisgroep Noord in kaart gebracht hoe mutaties nu worden gedocumenteerd. In 2019 zal Zonnehuisgroep Noorder verder onderzoek doen hoe alle belangrijke mutaties op de applicatie kunnen worden geregistreerd eventueel met behulp van een applicatie logboek. Centrale plaats realiseren voor documentenbeheer (contracten, SLA en dergelijke) per applicatie te gaan vastleggen. Verder is een verbeterpunt voor 2019 om ook informatie over de besluitvorming over updates en het testen hiervan beter vast te leggen. Het verbeterplan wordt in 2019 uitgevoerd door Zonnehuisgroep Noord.

Myobi (mind your own business)

Zonnehuisgroep Noord heeft zich aangesloten bij MYOBI, een Trusted Third Party (TTP) gericht op gegevensbescherming. Zonnehuisgroep Noord maakt gebruik van het privacy keurmerk van MYOBI (zie www.myobi.eu) om transparant te zijn over haar volwassenheidsniveau op het gebied van privacy en informatiebeveiliging. Door middel van volwassenheidsniveaus van het privacy keurmerk kan het bestuur accountable zijn voor het niveau van gegevensbescherming dat door Zonnehuisgroep Noord waargemaakt wordt. Het privacy keurmerk is onderverdeeld in zeven opeenvolgende niveaus. Door middel van een jaarlijks bestuurlijk gesprek tussen de professionals van MYOBI en het bestuur van de organisatie wordt vastgesteld wat het op dat moment geldende niveau van de organisatie is. In Q4 2018 heeft Zonnehuisgroep Noord niveau 3 bereikt en in Q4 2019 wil Zonnehuisgroep Noord niveau 4-5 bereiken.

Daarnaast sluit Zonnehuisgroep Noord via de TTP verwerkersovereenkomsten met partners in de keten. Door gebruik te maken van een gemeenschappelijk normenkader, datalek protocol en een mediation regeling wordt het veel eenvoudiger om verwerkersovereenkomsten af te sluiten. De aansprakelijkheden kunnen zo evenwichtiger verdeeld worden over de partijen en Zonnehuisgroep Noord is voorspelbaar in het netwerk.
In 2018 heeft Zonnehuisgroep Noord 22 verwerkersovereenkomsten afgesloten. We zijn met een aantal verbonden partijen in gesprek om een verwerkersovereenkomst af te sluiten. Hierbij lopen we tegen verschillende knelpunten aan. Vaak zijn partijen nog niet (volledig) op de hoogte van de nieuwe wetgeving en hebben ze hier nog geen visie op ontwikkeld. Andere partijen hebben zelf een verwerkingsovereenkomst opgesteld die of niet volledig is of nog gestoeld is op oude wetgeving. Zonnehuisgroep Noord zal in 2019 doorlopend en indien nodig verwerkersovereenkomsten afsluiten met nieuwe partijen en de verwerkersovereenkomsten afsluiten met bestaande partijen afronden. Eén van de afspraken die gemaakt wordt in de verwerkersovereenkomst is het aantonen van de effectieve werking van de organisatorische en technische maatregelen die genomen zijn. Zonnehuisgroep Noord doet dit door het ter beschikking stellen van deze DoA aan alle

ketenpartners. Tot nu toe hebben we nog geen bewijs van effectieve werking van ketenpartners ontvangen. In 2019 wil Zonnehuisgroep Noord hier strakker op gaan sturen en ketenpartners bewust maken van hun verantwoordelijkheid in dezen. Ook willen we de noodzaak bespreken dat verwerkers eveneens een privacy en security boekhouding voeren waardoor zij ook aantoonbaar auditable zijn aan de eisen van de Avg.

Website

Ook in 2019 wil Zonnehuisgroep Noord op de website uitdragen, dat ze een betrouwbare en voorspelbare partij is op het gebied van privacy en informatiebeveiliging. Vanaf 2017 is het privacy keurmerk opgenomen met de hyperlink naar Myobi. Zo zien betrokkenen hoe Zonnehuisgroep Noord omgaat met privacy en informatiebeveiliging. De Verklaring van Accountability plaatst Zonnehuisgroep Noord ook jaarlijks op de website.
in 2018 heeft Zonnehuisgroep Noord nog meer informatie gegeven over privacy op haar website, onderwerpen die toegevoegd zijn:

- In de privacyverklaring is onder andere opgenomen
  - Overzicht van alle verwerkingen en doelen;
  - Rechten van betrokkenen;
  - Mogelijkheid voor vragen / opmerkingen en klachten voor betrokkenen;
- Verklaring van Accountability (DoA)

In 2019 zal Zonnehuisgroep Noord het camerabeleid toevoegen en de informatie op de website blijven optimaliseren.

7. Ambitie voor 2019

Zonnehuisgroep Noord heeft de ambitie geformuleerd om eind 2018 op volwassenheidsniveau 3-4 van het privacy keurmerk te staan. Q4 2018 is niveau 3 bereikt. Voor 2019 heeft Zonnehuisgroep Noord de ambitie volwassenheidsniveau 4-5 te halen.

Er zijn noodzakelijke randvoorwaarden nodig om deze ambitie te realiseren:

- ICT strategie welke is uitgewerkt in 2018 moet in 2019 worden gerealiseerd;
- Beleggen operationele taken in de lijn; en
- Door verder de samenwerking met vergelijkbare organisaties neer te zetten en de afhankelijkheid en kwetsbaarheid van de FG te verminderen.
  (In 2018 heeft de FG van Zonnehuisgroep Noord het Regionaal Netwerk Functionaris Gegevensbescherming in het noorden opgezet)

Samengevat hebben wij voor 2019 de volgende doelstellingen benoemd:

- Implementeren e-learning / bewustwording programma en koppelen aan SBC applicatie
- Bewustwording medewerkers vergroten;
- Verwerkers bewust maken dat zij eveneens een privacy en security boekhouding voeren waardoor zij ook aantoonbaar auditable zijn aan de eisen van de Avg;
- Een transparant en vastgesteld autorisatiebeleid en daarnaast periodieke controles van de autorisaties op alle (kern)systemen;
- Implementatie Single Sign On (SSO);
- Webmail proces herzien en aanscherpen;
- Technische security maatregelen verbeteren;
- Inzet periodieke beveiligings- en penetratietesten;
- Inzetten controle autorisaties en continu monitoring (technische infrastructuur);
- Procedures proces in-door- en uitstroom, aanvraag account en proces aanvraag autorisatie externen aanscherpen;
- Belangrijke mutaties op de applicatie worden geregistreerd eventueel met behulp van een applicatie logboek en een centrale plaats realiseren voor documentenbeheer;
- Beter vastleggen van de besluitvorming over updates van systemen en het testen hiervan;
- Handhaving op de vernietigingstermijnen van gegevens optimaliseren;
- De rechten van alle betrokkenen zo volledig mogelijk blijven faciliteren;
- Informatiebeveiliging verwerken in het compliance (naleving) control framework;
- Op de website blijven uitdragen, dat Zonnehuisgroep Noord een betrouwbare en voorspelbare partij is op het gebied van privacy en informatiebeveiliging.
- Ter voorbereiding op de gespecificeerde toestemming van betrokkenen hiervoor het fundament faciliteren. De voorbereiding treffen van een bedrijfsspecifieke data gedreven omgeving naar een omgeving waar de betrokkene ‘in control’ is;

8. Samenvatting bestuursverslag

De tekst voor het bestuursverslag 2019 is op basis van het voorgaande samengesteld.

Gegevensbescherming & informatieveiligheid

Informatie, en in het bijzonder persoonsgegevens, komen in verschillende vormen in onze organisatie voor. De kwaliteit van deze informatie is essentieel voor een effectieve en een kostenefficiënte zorg. Wij hebben beleid op dit vraagstuk ontwikkeld en voeren het ook uit.

In snel tempo wordt wetgeving op het gebied van privacy en informatieveiligheid aangenomen. Het verplicht zorginstellingen hun gegevensbescherming en informatiebeveiliging op orde te brengen en te houden. Binnen het informatie- en privacybeleid hebben wij de wettelijke verplichtingen een plaats gegeven.

Zonnehuisgroep Noord vindt het belangrijk dat met de gegevens van een ander wordt omgegaan zoals iedereen zou willen dat er met de eigen persoonsgegevens wordt omgegaan. Dit betekent privacy bewustzijn bij iedere medewerker. Hierbij nemen we de volgende punten mee bij het maken van keuzes:

- Privacy en gegevensbescherming mag de zorg 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; en
- Zorgvuldigheid staat voorop maar het helemaal uitsluiten van datalekken is niet mogelijk.

Aan het maatschappelijk verkeer verantwoording afleggen over de realisatie en planning van het beleid hebben wij opgenomen in de gebruikelijke code good governance zorg. Begrippen 'Accountability' en 'Auditability' hebben een centrale plaats gekregen. Eind 2018 hebben wij een volwassenheidsniveau van 3 gehaald en over 2019 verwachten wij dat het volwassenheidsniveau op 4 - 5 ligt. Hiermee zijn wij transparant en laten wij een boven gemiddeld niveau in de sector zien.

In 2019 wordt gestart met het daadwerkelijk moderniseren van de informatiehuishouding. Het gaat er om een meer geïntegreerde gegevensverwerking te realiseren waardoor de kwaliteit van (persoons)gegevens stijgt en de operationele kosten dalen. Deze transformatie biedt kansen te voldoen aan de gespecificeerde toestemming voor verdere verwerking van persoonsgegevens en uiteindelijk de regie van persoonsgegevens bij de bewoner en medewerker te leggen.

Voor de “verklaring van accountability 2018” verwijzen wij naar onze website.