De Hoop ggz

Verklaring van accountability over de omgang met Persoonsgegevens in 2019

Verantwoording van De Hoop ggz aan stakeholders over het voldoen aan wet- en regelgeving op het gebied van privacy & informatiebeveiliging over 2019

Auteurs: Jaap de Gruijter, voorzitter Raad van Bestuur en Jan-Kees Obbink, Functionaris Gegevensbescherming

Datum: Mei 2020

Versie: 1.0

Voorwoord

Volgens artikel 4 lid 1 van de Algemene verordening gegevensbescherming (Avg) wordt onder het begrip persoonsgegevens verstaan: ‘alle informatie over een geïdentificeerde of identificeerde natuurlijke persoon’. Met andere woorden: persoonsgegevens betreffen ieder gegeven dat direct of indirect tot een persoon herleidbaar is, zoals naam, geboortedatum en BSN nummer. Ze komen in verschillende vormen voor, bijvoorbeeld op papier of elektronisch. Ze worden op verschillende wijze overgedragen: per post, via elektronische weg of ze worden mondeling uitgewisseld. Persoonsgegevens behoren op een veilige wijze te worden beschermd, rekening houdend met de vorm of de wijze waarop ze worden gedeeld en/of opgeslagen. Voor het omgaan met persoonsgegevens is verschillende wetgeving van toepassing.

Per 1 juli 2017 is het Besluit elektronische gegevensverwerking door zorgaanbieders in werking getreden. Dit besluit verplicht zorginstellingen om hun informatiebeveiliging conform de NEN normen in te richten:

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

Er zijn daarnaast veel wetten, besluiten en regelingen die de verwerking van persoonsgegevens regelen. De belangrijkste wetten waarop de AP toezicht houdt zijn de Algemene verordening gegevensbescherming (Avg) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAvg). De Avg is rechtstreeks van toepassing in Nederland en waar de Avg ruimte laat voor nationale keuzes bij de uitvoering van de Avg, zijn deze ingevuld in de Uitvoeringswet Avg (UAvg).

In de Avg is 'Accountability' een kernbegrip. Dit begrip houdt in dat organisaties en ondernemingen moeten kunnen aantonen dat zij compliant zijn. Zij moeten bijvoorbeeld kunnen laten zien dat op de juiste wijze om toestemming voor gegevensverwerking is gevraagd, en dat de juiste beveiligingsmaatregelen zijn getroffen. Middels deze verklaring verwacht De Hoop op de juiste wijze hierover verantwoording af te leggen met betrekking tot verslagjaar 2019.

Inhoudsopgave

1. Inleiding

1.1. Doel Verklaring van Accountability

De Avg eist van de verantwoordelijke dat hij verantwoording aflegt over de wijze waarop hij met persoonsgegevens omgaat (zie art. 5 lid 2 van de Avg). Middels dit document voldoet de Raad van Bestuur van De Hoop aan deze verantwoordingseis vanuit de Avg te voldoen.

In deze verklaring wordt beschreven hoe een organisatie als De Hoop 'in control' is en hoe de verplichtingen vanuit de wet- en regelgeving worden nageleefd.

1.2. Doelgroep

In deze verklaring wordt de ontwikkeling rondom privacy en informatiebeveiliging beschreven en welke rollen voor verschillende personen zijn weggelegd. De Functionaris Gegevensbescherming (FG) ziet toe op het privacybeleid van De Hoop en de uitvoering daarvan en geeft hierover adviezen aan de manager Beleid & Informatie en de Raad van Bestuur. Vanaf mei 2018 is binnen De Hoop ook een Security Officer (functionaris Informatiebeveiliging) aangesteld die zorgt voor een aantoonbare continue effectieve werking van beheer en beveiligingsmaatregelen met betrekking tot onze applicaties en het - samen met zijn collega's van IT - organiseren van deze maatregelen en de inrichting van de IT en processen.

Deze verklaring is een governance verklaring en is bestemd voor stakeholders (belanghebbenden) van De Hoop, zoals cliënten, medewerkers, leveranciers, financiers en andere geïnteresseerden. De controle op aspecten van privacy en informatiebeveiliging kan onderdeel zijn van de controle op de jaarrekening door de accountant. De accountant kan deze verklaring in dat verband meenemen in het vaststellen van zijn controleverklaring.

In de 'mededeling van de Raad van Bestuur' neemt de Raad van Bestuur de verantwoordelijkheid op zich voor deze verklaring en ondertekent deze ook. De FG spreekt zich uit over de omgang met persoonsgegevens en zijn nieuwe rol als FG binnen De Hoop.

2. Mededeling raad van bestuur

De Avg gaat over het recht op bescherming van persoonsgegevens. Dit is een positief recht, waarmee wordt bedoeld dat ieder individu het recht heeft dat informatie over hem of haar met respect wordt behandeld. En ieder individu daarbij recht heeft op inzage in persoonsgegevens die over hem of haar worden verwerkt. Hij of zij mag deze laten aanpassen, aanvullen of verwijderen en nagaan of de verwerking in lijn is met het doel waarvoor persoonsgegevens worden verwerkt. Tevens mag ieder individu volledige verwijdering van diens persoonsgegevens eisen en mag een vraag stellen aan de Functionaris Gegevensbescherming, indien hij of zij meent dat diens persoonsgegevens niet juist zijn verwerkt en/of onvoldoende zijn beschermd.

Hieruit vloeit voort dat we het bij De Hoop als belangrijke opdracht zien om persoonsgegevens van onze cliënten, medewerkers en vrijwilligers te beschermen en er zorgvuldig mee omgaan. Wij en met name onze medewerkers in de zorgverlening hebben immers dagelijks te maken met het (geautomatiseerd) verwerken van persoonsgegevens.

Zorgvuldigheid betrachten doen we niet alleen omdat het een wettelijke verplichting is, maar vooral omdat wij dat zelf erg belangrijk vinden en waar ik als bestuurder voor sta. Onze cliënten, medewerkers en vrijwilligers kunnen ervan uit gaan dat wij hun rechten niet schenden en dat wij zorgvuldig met hun persoonsgegevens omgaan. Dat begint bij bewustwording en resulteert als het in compliant zijn aan de regels van de Avg. Over de wijze waarop wij compliant zijn leggen we in deze verklaring verantwoording af.

Met de vervanging van de Wet bescherming persoonsgegevens door de Avg per 25 mei 2018 moesten we het bestaande privacybeleid verder aanscherpen. Er is in dat kader een Functionaris Gegevensbescherming (FG) aangewezen binnen De Hoop ggz en is tevens gestart met een certificeringstraject voor de NEN 7510, een belangrijke graadmeter voor de stand rondom Informatiebeveiliging binnen De Hoop ggz. Tot onze vreugde mochten we dat certificaat op 3 december 2018 in ontvangst nemen van DNVWij verwachten dat we dit certificaat na de komende externe audits in mei 2020 kunnen behouden.

Wij hopen en verwachten dat het ingezette privacybeleid kan worden voortgezet in de komende jaren, waarbij we steeds alert blijven op mogelijke privacyrisico's, maar ook nieuwe kansen. Deze risico's en kansen blijven we monitoren zodat we er op kunnen inspelen op een moment dat dit zinvol is. Dat blijft een uitdaging waar we van harte mee aan de slag gaan!

Jaap de Gruijter
Voorzitter Raad van Bestuur mei 2020

3. Mededeling Functionaris Gegevensbescherming

Begin 2018 was De Hoop ggz zich bewust dat in verband met de komende Avg een FG moest worden aangesteld. Nadat beoordeeld was of deze taak kon worden gedaan binnen mijn contracturen als beleidsmedewerker ben ik in april 2018 aangewezen als FG en heb me als zodanig aangemeld bij de Autoriteit Persoonsgegevens.

Sinds mei 2018 ben ik aangesloten bij de Nederlandse beroepsvereniging van Functionarissen voor Gegevensbescherming enga regelmatig naar de in dat kader georganiseerde bijeenkomsten . Dat is een waardevolle aanvulling, wat betreft kennisvermeerdering en kennisuitwisseling.

Mijn werk als FG heeft in 2019 hoofdzakelijk bestaan uit de dagelijkse check op mogelijke datalekken in ons VIM-systeem. Wanneer het naar mijn inschatting om een datalek ging die gemeld moest worden bij de AP heb aan onze voorzitter RvB geadviseerd dat zo te doen en - na diens akkoord - het lek gemeld bij de AP.
Ook doe ik een dagelijkse check op de specifieke mailbox voor privacygerelateerde vragen van cliënten en medewerkers van De Hoop, waar ik zo mogelijk diezelfde dag nog op reageer.

Daarnaast heb ik onderzoek gedaan – samen met andere betrokkenen – naar mogelijke privacyrisico's van nieuwe gegevensverwerking met een mogelijk hoog privacyrisico (de zogenaamde DPIA's), zoals bij ons nieuwe EPD dat naar verwachting medio 2020 in gebruik kan worden genomen.

Al met al een uitdagende functie waar ik me ook komende tijd voor wil blijven inzetten!

Jan-Kees Obbink mei 2020
Functionaris Gegevensbescherming

4. Vastleggen persoonsgegevens

De Hoop ggz heeft in haar privacyverklaring aangegeven welke persoonsgegevens zij verwerkt en de doelen waarvoor zij worden verwerkt en op basis van welke grondslag (bijvoorbeeld toestemming van de betrokkene). Tevens is aangegeven dat vragen over de omgang met persoonsgegevens bij De Hoop kunnen worden gesteld via privacy@dehoop.org. Deze verklaring is te vinden op de website van De Hoop via de link: https://www.dehoop.org/privacy-en-proclaimer/
Deze privacyverklaring is gebaseerd op het verwerkingsregister van De Hoop waarin per categorie van gegevensverwerking ook de bovenstaande zaken staan vermeld en tevens per verwerking de technische en organisatorische maatregelen om de betreffende persoonsgegevens te beveiligen. Dit register is in beheer bij de FG van De Hoop. Hiermee voldoen we aan belangrijke beginselen vanuit de AVG, zoals rechtmatigheid, transparantie, doelbinding en juistheid van de gegevensverwerkingen. Uit dit register blijkt onder andere dat vanuit De Hoop geen persoonsgegevens worden verstrekt aan landen buiten de Europese Unie (de zogenaamde 'derde landen').

5. Beleid

Het beleid van De Hoop ggz rondom privacy & informatiebeveiliging ligt vast in verschillende documenten waar een samenhang tussen bestaat. Hieronder is per document het doel en de voortgang omschreven.

Privacyreglement
. In 2019 is het in 2018 op de AVG aangepaste privacyreglement niet opnieuw gewijzigd.

Privacy & informatiebeveiligingsbeleid

In het kader van de NEN 7510 certificering zijn veel beleidsdocumenten opgesteld rondom het op een juiste wijze omgaan met persoonsgegevens van cliënten en medewerkers. Deze hebben hun weerslag gekregen in onze privacyverklaring die in mei 2018 is gepubliceerd op onze website. De laatste update is eind 2019 geweest op basis van de gewijzigde WGBO per 1-1-2020, waarbij de bewaartermijn van een medisch dossier is gewijzigd naar 20 jaar (was 15 jaar). Deze wordt jaarlijks geëvalueerd en zonodig aangepast op nieuwe ontwikkelingen op dit gebied. Er is naar aanleiding van de Avg een richtlijn Opvolging datalekken geschreven die intern vastlegt hoe moet worden gehandeld wanneer sprake is van een datalek. In dat verband hebben alle leidinggevenden van De Hoop een memo ontvangen die beschrijft wanneer sprake is van een datalek en wat de procedure is wanneer hiervan sprake is. Sindsdien worden er zeer regelmatig (mogelijke) datalekken gemeld via ons VIM-systeem. Wat betreft emails met gevoelige informatie is voorgeschreven dat dit via de methode Veilig Verzenden wordt gedaan en dat voorkomt datalekken.

Autorisatie en authenticatie beleid

Het autorisatiebeleid geeft aan wie waarvoor toegang heeft in een bepaalde applicatie en welke periodieke controle daarop plaatsvindt. De FG doet ieder kwartaal steekproefsgewijs een controle op niet reguliere toegang tot cliëntdossiers. Dat betreft toegang tot een cliëntdossier door een medewerker die geen behandelrelatie heeft met de betreffende cliënt, maar om hem of haar moverende redenen toch toegang nodig heeft. Deze toegang kan alleen worden verkregen na opgave van een reden waarom dat nodig is. Tevens geldt hierbij een sanctiebeleid dat zonodig kan worden toegepast wanneer er onnodig en na waarschuwing in een cliëntdossier wordt gekeken.
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. Indien medewerkers buiten de kantooromgeving Citrix willen benaderen is ook een code via SMS nodig (two way authenticatie).
De Hoop werkt met single-sign-on (SSO). Dat stelt medewerkers in staat om eenmalig in te loggen, waarna automatisch toegang wordt verkregen 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 de afdeling ICT. Daarnaast biedt De Hoop medewerkers de mogelijkheid om via webmail de mailbox te benaderen, waarbij geen toegang mogelijk is tot eigen of gedeelde bestanden.

Privacybeleid en gedragsregels

De Hoop heeft een Gedragscode Informatiebeveiliging die beschrijft op welke wijze vorm wordt gegeven aan vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Deze gedragscode heeft betrekking op medewerkers, stagiaires en vrijwilligers. De Hoop geeft geen persoonsgegevens door aan landen buiten de Europese Unie. We streven naar dataminimalisatie door alleen de relevante persoonsgegevens te verwerken en hierop bijvoorbeeld ook ons EPD te screenen. In ons archief liggen nog veel papieren cliëntdossiers en wij zijn deze nu systematisch aan het doorlopen, zodat alleen nog de dossiers die bewaard moeten blijven op grond van de bewaarplicht overblijven.

6. Awareness / risico inventarisatie

6.1 Awareness

De Hoop besteedt aandacht aan de bewustwording van medewerkers op het onderwerp privacy & informatiebeveiliging.
Alle medewerkers van De Hoop zijn opgeroepen om via GGZecadamy een digitale cursus Privacy en Informatiebeveiliging te doen. Ondertussen hebben circa 230 medewerkers een certificaat behaald.
Onderdeel van de awareness is ook het informeren van betrokkenen over hun rechten.
Deze rechten zijn vastgelegd in ons privacyreglement, waarbij voor cliënten nog een korte samenvatting ter beschikking staat via de folder Cliëntenrechten. Bij eventuele vragen is voor zowel cliënten als voor medewerkers het mailadres privacy@dehoop.org beschikbaar, waarna in het algemeen de FG de betreffende vraag zal kunnen beantwoorden.

6.2 Data Privacy Impact Analyse (DPIA) “gegevenseffectbeoordeling”

Mede naar aanleiding van een suggestie van de auditor in het kader van de NEN certificering is begin 2019 een DPAI gedaan op ons huidige EPD EZRA in aanwezigheid van de teamleider Functioneel

beheer, de externe projectleider vanuit BM Grip en de FG. Hier zijn geen onacceptabele risico's uit naar voren gekomen.. In oktober 2019 hebben dezelfde mensen bij De Hoop ook een DPIA gedaan van het nieuwe EPD User, dat medio 2020 in werking moet gaan treden. Naar aanleiding van deze DPIA zijn een drietal vragen gesteld aan de FG van de EPD-leverancier (Impulse) die middels een mail van 18-11-2019 naar tevredenheid zijn beantwoord.

6.3 Analyse van datalekken

Er zijn in 2019 38 datalekken gemeld via ons VIM-systeem, waarvan drie zijn gemeld bij de Autoriteit Persoonsgegevens (AP). Het betrof niet heel ernstige datalekken en de AP heeft hier ook geen nader onderzoek op gedaan. Het besluit over het wel of niet melden aan betrokkenen die door het datalek zijn benadeeld wordt in principe genomen in het zogenaamde crisisberaad datalekken na een gedane melding bij de AP.
De meldingen met betrekking tot mogelijke datalekken zijn van verschillende afdelingen afkomstig, wat erop duidt dat het melden hiervan goed bekend is bij de medewerkers. Gezien de eindverantwoordelijkheid van de Raad van Bestuur (RvB) voor de meldingen van datakekken is afgesproken dat met ingang van december 2018 de RvB het besluit neemt tot wel of niet melden van een datalek, na advies van de FG hierover. Dat is in 2019 op die wijze gedaan.

6.4 Onderzoeken

Bij de laatste AP-melding is een intern beraad geweest met de direct betrokken medewerkers, onder leiding van de manager Beleid & Innovatie, om zo mogelijk verbetermaatregelen vast te stellen en vervolgens te implementeren. Bij de andere twee datalekken werd dat minder noodzakelijk geacht omdat de interne melder van het datalek zelf al de betrokkenen had geïnformeerd.

6.5 Checklist aanschaf nieuwe applicatie

De Hoop gaat in 2020 onderzoeken of bij aanschaf van een nieuwe applicatie een checklist gebruikt kan worden om te zorgen, dat de betreffende applicatie in ieder geval voldoet aan geldende wet- en regelgeving op het gebied van privacy en informatiebeveiliging.
Deze checklist zou er als volgt uit kunnen komen te zien:

- Het voor afsluiten contract doen van een Data Privacy Impact Analyse (DPIA)
- Het afsluiten van een verwerkersovereenkomst voor aanvang gegevensverwerking
- Check op het voldoen aan de uitgangspunten vanuit het pakket van eisen (PvE), bijvoorbeeld het hebben van een NEN 7510 certificaat
- Doen van periodieke controles op autorisaties ten behoeve van verwerkers
- Centrale opslag van contracten, service level agreements en andere afspraken met de leverancier in Ultimo.

6.6 Samenwerken met ketenpartners die zelf verwerkingsverantwoordelijke zijn

De Hoop werkt met een aantal ketenpartners samen die vanwege hun eigen verantwoordelijkheid wat betreft het bepalen van doel en middelen met betrekking tot de gegevensverwerking, naast De Hoop zelfstandig verwerkingsverantwoordelijke zijn. In 2019 betrof dat onze apotheker (Benu apotheek te Dordrecht), Stichting De Brug te Katwijk en Profila Zorg te Houten.

7. Ambities voor 2020

De Hoop heeft als ambitie voor 2020 om haar NEN 7510 certificaat te behouden. De hiervoor benodigde audits worden zoveel mogelijk gecombineerd met de benodigde HKZ-audits, zodat de auditees maar één keer worden bevraagd voor twee certificeringen.
Ook zal aan de awareness bij medewerkers weer de nodige aandacht besteed worden, waarbij nog wordt onderzocht op welke wijze dat het beste gedaan kan worden. Wellicht door in de periodieke Informail aandacht aan dit onderwerp te besteden of door opnieuw een (nep) phishing mail rond te laten gaan.