De Hoop

Verklaring van accountability over de omgang met Persoonsgegevens in 2023

Verantwoording van De Hoop aan stakeholders over het voldoen aan wet- en regelgeving op het gebied van privacy & informatiebeveiliging over 2023

Auteurs: Irene Blom en Paul Vel Tromp (Raad van Bestuur), Jan-Kees Obbink (Functionaris Gegevensbescherming) en Eline van Veluw (Functionaris Informatiebeveiliging)

Datum: februari 2024

Versie: definitief

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 de Wet cliëntenrechten bij elektronische verwerking van gegevens in werking getreden. Een zorgverlener is daarmee verplicht om zijn cliënt te informeren over de elektronische gegevensuitwisseling en toestemming te vragen voor het beschikbaar stellen van de cliëntgegevens via een elektronisch uitwisselingssysteem. Vanaf 2020 kan de cliënt bovendien aangeven welke gegevens wel of niet door welke (categorieën van) zorgverleners mogen worden ingezien (gespecificeerde toestemming). Voor alle duidelijkheid: het gaat altijd uitsluitend om zorgverleners waarmee de cliënt (dan) een behandelrelatie heeft. Andere zorgverleners mogen zijn gegevens niet zien. Verder heeft de patiënt het recht op (gratis) elektronische inzage in zijn dossier en recht op een elektronisch afschrift daarvan.

Per 1 januari 2018 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).
- NTA 7516: veilig mailen in de zorg: NTA 7516 beschrijft in techniek neutrale termen de eisen waaraan e-mail, met daarin patiëntgegevens, zou moeten voldoen om veilig te zijn. Het gaat daarbij enerzijds om de waarden die geborgd moeten worden, zoals de mate van beschikbaarheid, integriteit en vertrouwelijkheid, maar ook gebruiksvriendelijkheid. Dit laatste is een belangrijk uitgangspunt, om ervoor te zorgen dat oplossingen voor veilige mail ook daadwerkelijk gebruikt gaan worden.

De Wet elektronische gegevensuitwisseling (Wegiz) in de zorg is op 1 juli 2023 in werking getreden. Het doel van de Wegiz is om de wijze van gegevensuitwisseling tussen zorgverleners te uniformeren, zodat niet iedereen een ‘andere taal spreekt’. Het idee is dat zorgverleners hierdoor (tijdig) de beschikking krijgen over adequate, actuele en uniforme gegevens over de cliënt wanneer dit nodig is.

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 2023.

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

In deze verklaring wordt beschreven hoe 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 medewerkers en cliënten binnen De Hoop, alsmede de divisiemanager Serviceorganisatie en de Raad van Bestuur. Vanaf mei 2018 is binnen De Hoop ook een Security Officer (Functionaris Informatiebeveiliging, ook wel FIB) aangesteld die zorgt voor een aantoonbare, continue, effectieve werking van beheer en beveiligingsmaatregelen met betrekking tot onze applicaties. En deze organiseert - samen met collega's van ICT – dat deze maatregelen worden ingericht in de ICT-systemen en -processen. De Functionaris Informatiebeveiliging heeft ook bijgedragen aan het opstellen van deze verklaring.

Deze verklaring is een governance verklaring en is bestemd voor interne en externe stakeholders 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 binnen De Hoop en de FIB over de ontwikkelingen / bijzonderheden met betrekking tot Informatiebeveiliging.

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 persoonlijke informatie over hem of haar met respect wordt behandeld. En ieder individu heeft recht heeft op inzage in persoonsgegevens die over hem of haar worden verwerkt, anders dan voor persoonlijk gebruik. 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 zijn 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 om te gaan. 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 intrinsiek belangrijk vinden en daar willen wij als Raad van Bestuur voor staan. 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 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 en is tevens gestart met een certificeringstraject voor de NEN 7510, een belangrijke graadmeter voor de stand rondom Informatiebeveiliging binnen De Hoop. Tot onze vreugde mochten we dat certificaat op 3 december 2018 in ontvangst nemen van DNV. Hierna hebben we ieder jaar de externe audits met goed gevolg doorstaan en wij verwachten dat we dit certificaat na de komende externe audit in september 2024 ook weer kunnen behouden. In 2020 is de FIB rol verder geformaliseerd binnen De Hoop waarmee de informatiebeveiliging steviger is gepositioneerd binnen De Hoop.

De Hoop besteedt serieus aandacht aan cybersecurity. We zijn ons bewust van de hedendaagse risico's, en in navolgende wordt beschreven welke maatregelen we in hebben gezet.

Wij hopen en verwachten dat het ingezette privacy en informatiebeveiligingsbeleid kan worden voortgezet in de komende jaren, waarbij we steeds alert blijven op mogelijke privacy en informatiebeveiligingsrisico's, maar ook op 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 verder mee aan de slag gaan!

Irene Blom
Voorzitter Raad van Bestuur

Paul Vel Tromp
Lid Raad van Bestuur

Februari 2024

3. Mededeling Functionaris Gegevensbescherming

Begin 2018 was De Hoop 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 en ga regelmatig naar de in dat kader georganiseerde bijeenkomsten. Dat is een waardevolle aanvulling, wat betreft kennisvermeerdering en kennisuitwisseling.

Mijn werk als FG heeft in 2023 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 Autoriteit Persoonsgegevens (AP) heb ik aan onze voorzitter RvB geadviseerd dat zo te doen en - na diens akkoord - het lek gemeld bij de AP. Daarnaast doe ik een dagelijkse check op een specifieke mailbox voor privacy-gerelateerde vragen van cliënten en medewerkers van De Hoop, waar ik zo mogelijk diezelfde dag nog op reageer.
Zowel medewerkers als cliënten van De Hoop weten deze mailbox steeds vaker te vinden, wat erop wijst dat het thema privacy breed bekend is en goed bekend is binnen De Hoop.

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

Jan-Kees Obbink *februari 2024*
Functionaris Gegevensbescherming

4. Mededeling Functionaris Informatiebeveiliging

Sinds medio 2020 is informatiebeveiliging bij twee personen belegd. In mijn rol coördineer ik de beleidsmatige, brede aspecten. De (ict) technische informatiebeveiligings aandachtgebieden zijn belegd bij de operationeel beheerder ICT. Vanuit mijn beleidsmatige ervaring ervaar ik het als een mooie uitdaging om Informatiebeveiliging verder op de kaart te zetten binnen De Hoop.
In 2023 is er toegewerkt naar een specifieke aanpak om bewustwording over informatiebeveiliging te vergroten. Ook is de opzet van interne audits doorontwikkeld, waarmee beter wordt aangesloten bij de praktijk van alledag. Daarnaast is steeds alert gereageerd op landelijke signalen m.b.t. informatiebeveiligingsrisico's en zijn waar nodig systemen aangepast en updates doorgevoerd. Tot slot werden landelijke ontwikkelingen zoals NIS2 nauwlettend gevolgd.

Eline van Veluw *februari 2024*
Functionaris Informatiebeveiliging

5. Vastleggen persoonsgegevens

De Hoop 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’).

6. Beleid

Het beleid van De Hoop 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 2023 is het in 2018 op de AVG aangepaste privacyreglement niet 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 zo nodig 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 e-mails met gevoelige informatie is voorgeschreven dat dit via de methode Veilig Verzenden wordt gedaan en dat voorkomt datalekken. Dit sluit aan bij de NTA 7516.
In 2023 is een herziening gedaan van protocol clear screen clean desk.

Interne audit 2023
In 2023 is een nieuw auditplan opgesteld, dat nog moet worden goedgekeurd/vastgesteld. In 2023 is geen auditronde gehouden; alle onderwerpen waren al getoetst in de afgelopen drie jaar en het was dus niet noodzakelijk om dit ook weer te doen in 2023.

Autorisatie- en authenticatiebeleid
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 zo nodig kan worden toegepast wanneer er onnodig en na waarschuwing in een cliëntdossier wordt gekeken. We zijn ons ervan bewust dat er een verdergaande toegangscontrole nodig is en dit is momenteel in onderzoek bij onze afdeling ICT

hoe dit vorm te geven. De AP heeft hierover aangegeven dat het om een systematische en consequente controle moet gaan van alle logging mbt EPD-toegang.

Authenticatie is het proces waarbij nagegaan wordt of iemand echt is wie hij beweert te zijn. Voor het beveiligd middels VPN inloggen op het Netwerk wordt gebruik gemaakt van gebruikersnaam en een sterk wachtwoord dat periodiek gewijzigd moet worden. Indien medewerkers buiten de kantooromgeving het netwerk van De Hoop willen benaderen is ook een code via SMS nodig (twee factor authenticatie). Op dit moment wordt onderzocht hoe we ook op kantoor deze twee factor authenticatie kunnen gaan toepassen.
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.

7. Awareness / risico inventarisatie

7.1 Awareness

De Hoop besteedt aandacht aan de bewustwording van medewerkers op het onderwerp privacy & informatiebeveiliging. Alle medewerkers van De Hoop zijn opgeroepen om via GGZ Ecademy een digitale cursus Privacy en Informatiebeveiliging te doen. Geborgd is dat iedere nieuwe medewerker gevraagd wordt deze cursus te doen. Hierop wordt ook actief navraag gedaan bij de leidinggevenden. 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. Aan de hand van een opgestelde planning wordt periodiek bewust aandacht geschonken aan informatiebeveiligingsonderwerpen vanuit de FG of de FIB.

7.2 Data Privacy Impact Analyse (DPIA) “gegevenseffectbeoordeling”

In 2023 is een DPIA gedaan op een proactieve beschermingsmodule, die verdachte digitale activiteiten van medewerkers kan detecteren en hierover een signaal kan afgeven aan onze ICT-afdeling. Volgens een in onze gedragscode Informatiebeveiliging vastgelegde procedure kan er vervolgens onderzoek naar worden gedaan, indien nodig. De DPIA heeft uitgewezen dat werken hiermee verantwoord is.

7.3 Analyse van datalekken

Er zijn in 2023 78 datalekken gemeld via ons VIM-systeem, waarbij het niet nodig was om te melden bij de AP. Het besluit over het wel of niet melden aan betrokkenen die door het datalek zijn benadeeld wordt in principe genomen in het zogenaamde opvolgend actieoverleg na melding datalekken. Regelmatig heeft de melder echter zelf al excuses gemaakt aan de betrokkene en dan is het opvolgend overleg hiervoor niet meer nodig.
De meldingen met betrekking tot datalekken zijn van verschillende afdelingen afkomstig, wat erop duidt dat het melden hiervan goed bekend is bij de medewerkers.

7.4 Checklist aanschaf nieuwe applicatie

De Hoop heeft in 2023 bij de aanschaf van de hiervoor genoemde beveiligingsmodule van CyberHunter gecheckt of de betreffende module in ieder geval voldoet aan geldende wet- en regelgeving op het gebied van privacy en informatiebeveiliging.

Deze checklist ziet er als volgt uit:

- Het voor afsluiten van een contract doen van een Data Privacy Impact Analyse (DPIA), indien nodig
- Het afsluiten van een verwerkersovereenkomst voor aanvang gegevensverwerking, indien nodig
- 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.

Achtergrond van deze nieuwe beveiligingsmodule

Dit betreft een programma dat het computergedrag van medewerkers op de achtergrond monitort en dat verdachte handelingen signaleert en onder de aandacht brengt van ICT. Dat gaat bijvoorbeeld om gebruik van een besmette USB stick in een apparaat van De Hoop, het niet regulier inloggen op het netwerk van De Hoop vanuit het buitenland of afwijkende patronen in computergebruik. Als het programma een dergelijke bedreiging signaleert kan ICT hiernaar een onderzoek instellen en de bedreiging uitschakelen. In de huidige situatie zou het gevaar pas worden ontdekt nadat de schade is aangericht, maar nu is de kans groter dat het ontdekt wordt voordat er schade wordt aangericht.

7.5 Check op clear desk en clear screen

Eigenaarschap/verantwoordelijkheid voor dit onderwerp is in de lijn belegd. Hiervoor is in 2023 aandacht gevraagd in de nieuwsbrief management.

7.6 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 2023 betrof dat onze apotheker (Benu apotheek te Dordrecht) en Stichting De Brug te Katwijk.

7.7 Inventarisatie cybersecurity risico's

In 2023 is er 3x een malwaremelding gedaan vanuit onze beveiligingsleverancier. Deze malware is preventief geblokkeerd. Er hebben zich (voor zover wij weten) geen DDOS-aanvallen voorgedaan. Het kan overigens zo zijn dat onze internetprovider deze aanvallen proactief geblokkeerd heeft, en daar krijgen wij geen melding van. Afgelopen twee maanden hebben we 11 "high criticals" opgelost in het netwerk. Gezien het voorgaande is onze organisatie in 2023 geen enkele keer in gevaar geweest. Dat is mede te danken aan onze beveiligingsleveranciers die meekijken en (snel) een signaal aan ons doorgeven, mocht er iets niet in orde zijn. Daarnaast hebben we preventieve maatregelen genomen die een aanval met malware zoveel mogelijk beperken.

8. Ambities voor 2024

In 2024 is onze ambitie om het NEN-certificaat te behouden (hercertificiering vindt dit najaar plaats). Met behulp van een nieuwe opzet van de interne audits willen we het eigenaarschap hiervan in de organisatie vergroten. Er zal dit jaar veel aandacht zijn voor bewustwording met betrekking van informatieveiligheid (door middel van uitvoering van het communicatieplan maar ook door regelmatige phishing acties).