# De Hoop ggz

# Verklaring van accountability over de omgang met Persoonsgegevens in 2021

Verantwoording van De Hoop ggz aan stakeholders over het voldoen aan wet- en regelgeving op het gebied van privacy & informatiebeveiliging over 2021

*Auteurs: Irene Blom (voorzitter Raad van Bestuur), Jan-Kees Obbink (Functionaris Gegevensbescherming) en Bram Paul Speelman (Functionaris Informatiebeveiliging)*

*Datum: januari 2022*

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 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.

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 2021.

# 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 de directeur Beleid & Informatie 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 hij organiseert - samen met zijn collega's van IT – dat deze maatregelen worden ingericht in de IT-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 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 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 intrinsiek belangrijk vinden en daar wil ik als bestuurder 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 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 DNV. Wij verwachten dat we dit certificaat na de komende externe audits in mei 2022 kunnen behouden. In 2020 is de FIB rol verder geformaliseerd binnen De Hoop waarmee de informatiebeveiliging steviger is gepositioneerd binnen De Hoop.

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 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!

*Irene Blom*
*Voorzitter Raad van Bestuur* *januari 2022*

## 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 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 2021 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.
Ook doe ik een dagelijkse check op de 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* *januari 2022*
*Functionaris Gegevensbescherming*

## 4. Mededeling Functionaris Informatiebeveiliging

De informatiebeveiliging was in de jaren tot medio 2020 belegd bij meerdere personen. De beleidsmatige aspecten waren belegd bij de afdeling beleid. De (ict) technische informatiebeveiliging aandachtgebieden waren en blijven belegd bij de teammanager operationeel beheer ICT. Tot medio 2020 liet De Hoop zich ook extern adviseren door BM-Grip. Met mijn komst als beleidsmedewerker heb ik de rol van Functionaris informatiebeveiliging op mij genomen en coördineer de beleidsmatige, De Hoop brede Informatiebeveiligingsvraagstukken. Vanuit mijn beleidsmatige ervaring en brede ICT ervaring ervaar ik het als een uitdaging om Informatiebeveiliging verder vorm te geven aan de hand van de gedegen basis die er nu al ligt gezien ook de met goed gevolgde uitgebreide certificering Nen 7510 in 2021. In 2021 is op basis van de meerjarenplanning interne audits uitvoering gegeven aan de interne audits. Tevens is eruitvoering gegeven aan de bewustwording informatiebeveiliging (gebaseerd op de planning 2020-2021) . In 2021 is De Hoop ggz aangesloten bij Z-Cert als onderdeel van een initiatief van de Nederlandse GGZ. Daarnaast is steeds alert gereageerd op landelijke signalen mbt informatiebeveiligingsrisico's en zijn waar nodig was systemen aangepast en zijn update doorgevoerd.

*Bram Paul Speelman* *januari 2022*
*Functionaris Informatiebeveiliging*

## 5. 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').

## 6. 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 2021 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.

Interne audit 2021
In 2021 zijn 2 audits met in totaal 11 afdelingen intern geaudit, dit conform de hiervoor opgestelde meerjarenplanning (). Bij elke audit wordt een rapportage verslag opgesteld en ter controle aan de auditee voorgelegd. Aan de hand van deze rapportageformulieren is per auditronde één overall rapportage opgesteld die met directeur Beleid & Innovatie, manager ICT en teamleider Operationeel Beheer is besproken. Naar aanleiding van beiden besprekingen na elke audit ronde (voor- en najaar 2021) is de rapportage aangepast en zijn de acties beschreven en ook toegewezen. Vervolgens zijn beiden ingebracht in het DT. Aan beiden verslagen is nadien de verwijzing naar SMS (SmartManSys) verwerkt en is die versie ook aan SMS toegevoegd De afwijkingen zijn expliciet in SMS opgenomen en hier wordt in 2022 actie op ondernomen. Ten aanzien van de genoemde verbeterpunten zijn een aantal reeds in gang gezet en een aantal zullen worden geprioriteerd voor de verbeterkalender ICT in de komende jaren.

Autorisatie en authenticatie beleid
Het autorisatiebeleid geeft aan wie waarvoor toegang heeft in een bepaalde applicatie en welke periodieke controle daarop plaatsvindt.
Mede naar aanleiding van een klacht over ons **autorisatiebeleid** zijn we een verbetertraject ingegaan om per functie binnen De Hoop vast te stellen welke autorisaties er nodig zijn binnen het EPD om de noodzakelijke werkzaamheden te kunnen doen.

De FG doet in principe 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. In november 2020 heeft De Hoop een nieuw EPD gekregen en de rapportage die nodig is voor deze controle is ondertussen operationeel. We zijn ons ervan bewust dat er een verdergaande toegangscontrole nodig is. De AP heeft hierover aangegeven dat het om een systematische en consequente controle moet gaan van alle logging mbt EPD-toegang. We zijn momenteel te onderzoeken hoe we dit vorm kunnen geven, wellicht middels een te ontwikkelen tool.

**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 GGZecadamy 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 informatiebeveiligingonderwerpen. Er is op initiatief van de FIB en de FG een opfriscursus gegeven aan de aandachtsfunctionarissen Kwaliteit & Veiligheid, waar een aantal relevante vragen naar voren kwamen en waar positieve feedback op is gekomen. Aanbeveling is om dit jaarlijks te herhalen.

## 7.2 Data Privacy Impact Analyse (DPIA) “gegevenseffectbeoordeling”

In 2020 is het nieuwe EPD in gebruik genomen, waarop voorafgaand aan de ingebruikname een aantal vragen aan de leverancier zijn gesteld, die naar tevredenheid zijn beantwoord.

## 7.3 Analyse van datalekken

Er zijn in 2021 59 datalekken gemeld via ons VIM-systeem, waarvan drie zijn gemeld bij de 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. Regelmatig heeft de melder zelf al excuses gemaakt aan de betrokkene.

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.

### 7.4 Checklist aanschaf nieuwe applicatie

De Hoop heeft in 2021 bij de aanschaf van een nieuwe applicatie gecheckt of de betreffende applicatie 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.

### 7.5 Check op cleardesk en clearscreen

In voorjaar 2021 heeft er een herziening van het clearscreen, cleandesk beleid plaatsgevonden. Waar voorheen minder expliciet was vastgelegd op welke wijze gedurende het jaar de controle kon worden uitgevoerd is in de herziene beschrijving hier veel aandacht aan besteed en zijn er instructie opgesteld hoe een toets uit te voeren.
Dit najaar heeft een uitgebreide onaangekondigde check op clearscreen, clean desk plaatsgevonden, op alle poli's behalve Vlissingen en Dordrecht. Door de lockdown aan het einde van 2021 is het helaas niet gelukt om de 2 resterende poli's en de hoofdlocatie in Dordrecht te bezoeke.n De locaties die zijn bezocht door de FIB zijn uitgebreid onderworpen aan clearscreen en cleandesk toepassing. Ook is het gesprek met diverse medewerkers op de locaties gevoerd om de noodzaak van clearscreen en cleandesk te onderstrepen. Van alle bezoeken zijn verslagen gemaakt en deze zijn gedeeld met de leidinggevenden. Belangrijk aandachtspunt blijft het cleandesk beleid en hoe om te gaan met werkgerelateerde aantekeningen. Tot slot is er nav het clearscreen cleandesk beleid ook extra aandacht geweest voor veilig werken van huis uit.

### 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 2021 betrof dat onze apotheker (Benu apotheek te Dordrecht), Stichting De Brug te Katwijk en Profila Zorg te Houten (deze samenwerking is medio 2021 gestopt).

## 8. Ambities voor 2022

De Hoop heeft als ambitie voor 2022 om haar NEN 7510 certificaat te behouden. De hiervoor benodigde audits worden qua planning zoveel mogelijk gecombineerd met de benodigde HKZ-audits, zodat de auditees maar één keer worden bevraagd voor twee certificeringen. Dit geldt met name voor de externe toetsing. Bij de interne audits - die ook dit jaar twee keer worden uitgevoerd - wordt afgestemd dat afdelingen niet een HKZ audit én een NEN audit ondergaan, vanwege de tijdinvestering voor beide onderwerpen.
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. Onder andere door op intranet regelmatig aandacht aan dit onderwerp te besteden en/of door opnieuw een (nep) phishing mail rond te laten gaan.
Daarnaast willen we graag verder komen op het onder punt 6 genoemde autorisatie- en authenticatiebeleid, met name ten aanzien van de daar genoemde knelpunten.