17/32

Uitspraak van het College van Toezicht van het Nederlands Instituut van Psychologen.

Het College van Toezicht van het Nederlands Instituut van Psychologen, hierna te noemen het College, heeft het volgende overwogen en beslist ten aanzien van de bij brief van 26 november 2017 door mevrouw A, hierna te noemen klaagster, ingediende klacht tegen de heer drs. B, hierna te noemen verweerder, lid van het Nederlands Instituut van Psychologen, en ingeschreven in het NIP-register A&O psycholoog NIP en in het NIP-register psycholoog NIP.

I Het verloop van de procedure

Het College heeft kennisgenomen van:

- het klaagschrift met bijlagen d.d. 26 november 2017;
- het verweerschrift met bijlagen d.d. 18 januari 2018;
- de repliek met bijlagen d.d. 19 februari 2018;
- de dupliek d.d. 22 maart 2018.

De behandeling van de klacht heeft buiten aanwezigheid van partijen plaatsgevonden ter zitting van het College van 18 april 2018.
Aldaar heeft het College besloten advies in te winnen bij een deskundige.
Het verzoek om advies is voorgelegd aan de heer C, deskundige op het gebied van ICT, informatiebeveiliging en privacy, en werkzaam bij het NIP als adviseur met betrekking tot de AVG.

De volgende stukken zijn vervolgens aan het dossier toegevoegd:

- het advies d.d. 4 juni 2018 van de heer C;
- de brieven d.d. 12 juli 2018 van de secretaris van het College aan partijen, waarin zij hen in kennis stelt van dit advies en hen in de gelegenheid stelt hierop te reageren, waarbij eerst de reactie van klaagster wordt gevraagd en daarna de reactie van verweerder;
- de brief d.d. 5 september 2018 van de secretaris van het College aan klaagster, waarin zij schrijft dat zij er, onder meer gelet op het telefoongesprek dat klaagster op 30 augustus 2018 had met de secretaresse van het College, vanuit gaat dat klaagster afziet van het geven van een reactie;
- de brief d.d. 25 september 2018 van verweerder, waarin hij reageert op het advies van de heer C.

Het College heeft de beraadslaging vervolgens voortgezet, hetgeen tot de onder VI verwoorde beslissing heeft geleid.

II De feiten

Op grond van de stukken kan van het volgende worden uitgegaan.

II 1. Klaagster heeft op 22 november 2017 in het kader van een sollicitatie een assessment gedaan bij verweerder.

II 2. Op 23 november 2017 heeft verweerder het conceptrapport van het assessment per e-mail als PDF document aan klaagster gezonden.

II 3. Op 27 november 2017 heeft klaagster een e-mail aan verweerder gestuurd, waarin zij hem meedeelt dat zij een klacht heeft ingediend bij het College, met betrekking tot de procedure en afhandeling van het assessment, omdat verweerder naar haar mening nalatig is geweest in het omgaan met haar vertrouwelijke gegevens betreffende het assessment.

II 4. Verweerder heeft klaagster per e-mail van 29 november 2017 geantwoord, waarop klaagster op 1 december 2017 per e-mail heeft gereageerd.

III Het standpunt van klaagster en de klacht

De klacht houdt in, zakelijk weergegeven, dat verweerder in strijd met de Beroepscode heeft gehandeld om de volgende redenen.

1. Klaagster verwijt verweerder dat hij het conceptrapport als onbeveiligd PDF document via onbeveiligde e-mail aan haar heeft gezonden.
   Volgens klaagster heeft verweerder na het eerste conceptrapport nog tweemaal op dezelfde onbeveiligde wijze een herziene versie van het rapport naar haar e-mailadres verstuurd.
   Ook is het definitieve rapport onbeveiligd per e-mail naar de opdrachtgever gezonden, aldus klaagster.
   Klaagster zegt te beschikken over een schriftelijke verklaring van de opdrachtgever waarin deze dat bevestigt.
   Klaagster stelt dat verweerders handelwijze in strijd is met geldende wetgeving op het gebied van bescherming van persoonsgegevens, met de Beroepscode en met de *'Vuistregels beveiliging digitale cliëntendossiers'* die op de website van het NIP staan.
   Volgens klaagster strookt deze gang van zaken evenmin met het op de website van het bureau van verweerder vermelde privacyreglement.

2. Volgens klaagster werd haar voor het assessment gevraagd haar adresgegevens aan verweerders bureau te mailen. Klaagster acht haar adres niet relevant voor het afnemen van het assessment, aangezien zij niets per post heeft ontvangen, maar er uitsluitend via e-mail is gecorrespondeerd.

3. Klaagster stelt dat, toen zij aan het einde van de assessmentdag haar laatste opdracht wilde inleveren, de contactpersoon al naar huis bleek te zijn gegaan, zodat zij haar opdracht moest inleveren bij de enige nog in het pand aanwezige persoon, hetgeen haar geen prettig gevoel gaf.

IV Het standpunt van verweerder

Verweerder heeft de klacht gemotiveerd betwist en daartoe onder meer, zakelijk weergegeven, het volgende gesteld.

<u>Ad klachtonderdeel 1:</u>

Volgens verweerder heeft hij bij de systeembeheerder nagevraagd of de e-mailcorrespondentie veilig was verlopen, waarop deze een analyse daarvan heeft gemaakt, die in het verweerschrift is geciteerd, en waarvan de conclusie als volgt luidde: *"Kijkend naar bovenstaande punten dan is de communicatie via e-mail op een zo veilig mogelijke manier verlopen."*
Verweerder stelt dat niettemin inmiddels op zijn kantoor is afgesproken dat privacygevoelige documenten zullen worden versleuteld en zullen worden voorzien van een wachtwoord dat apart verstuurd wordt.

<u>Ad klachtonderdeel 2:</u>

Verweerder stelt dat het secretariaat van zijn kantoor de adresgegevens opvraagt voor het geval communicatie via e-mail niet mogelijk is, hetgeen een gerechtvaardigd doel is.
Het stond klaagster vrij om haar adresgegevens niet te verstrekken of om te vragen deze uit de administratie te verwijderen, hetgeen zij niet heeft gedaan, aldus verweerder.

Ad klachtonderdeel 3:

Volgens verweerder wordt er altijd voor gezorgd dat er tenminste een medewerker in het pand aanwezig blijft om stukken van kandidaten in ontvangst te nemen, eventuele vragen te beantwoorden en om kandidaten uitgeleide te doen.
Verweerder zegt in toekomstige situaties kandidaten daarover nog beter te zullen informeren.

V De overwegingen van het College

Ten aanzien van de klacht overweegt het College als volgt.

Ad klachtonderdeel 1:

V 1. Ten aanzien van het in dit klachtonderdeel gestelde heeft het College advies ingewonnen bij de heer C.

Het advies luidt als volgt:

"Op woensdag 25 april 2018 heeft T. Leenhouts, Secretaris College van Toezicht NIP, de volgende casus voorgelegd en daarbij behorende vragen gesteld:

Casus
Klaagster stelt dat de psycholoog het conceptrapport naar aanleiding van een assessment dat zij bij de psycholoog heeft ondergaan in het kader van een sollicitatie, als onbeveiligd PDF document via onbeveiligde e-mail aan haar heeft gestuurd. Zij acht dit getuigen van 'onzorgvuldig omgaan met mijn persoonlijke en vertrouwelijke gegevens'. Zij verwijst naar de 'Vuistregels beveiliging digitale cliëntendossiers van het NIP (zie de website van het NIP), naar de Beroepscode van het NIP en naar de WBp.

De psycholoog zegt dat hij het rapport als PDF document naar het door klaagster opgegeven e-mailadres heeft gezonden.
Hij heeft bij de systeembeheerder van zijn bureau nagevraagd of de e-mail beveiligd was.
Daarop heeft de systeembeheerder het volgende laten weten:

"De e-mail werd verstuurd via een beveiligde Exchange server welke voorzien was van alle op dat moment beschikbare beveiligingsupdates.
Communicatie met de e-mailserver is verlopen via een beveiligde verbinding en ook via het eigen bedrijfsnetwerk. De server waar Exchange op geïnstalleerd is, was op dat moment beveiligd met een sterk wachtwoord en voorzien van de meest recente Windows updates en antivirus software. De internet- en netwerkverbinding naar de server was afgeschermd middels een firewall. Verder is er een SPF (DNS) record beschikbaar waarmee een e-mailontvanger kan vaststellen of een e-mail van de juiste server afkomstig is. Dit om spoofing te voorkomen. De e-mail is verzonden via een e-mailprogramma dat alleen beschikbaar is na het inloggen op een met een wachtwoord beveiligd werkstation.
De werkstations en geïnstalleerde software zijn voorzien van de laatste updates (Windows en Office).

Kijkend naar bovenstaande punten dan is de communicatie via e-mail op een zo veilig mogelijk manier verlopen".

Het College is van oordeel dat voor de beantwoording van de vraag of de privacy al dan niet is geschonden, deskundigheid op het gebied van digitale informatieverstrekking is vereist. Om deze reden wordt de vraag aan u voorgelegd.

Vragen
Het College ontvangt graag antwoord op de volgende vragen:

1. Welke expliciete mogelijkheden zijn er om dergelijke documenten beveiligd te versturen?
2. Heeft de psycholoog voldaan aan de vereisten om maximale vertrouwelijkheid te garanderen?

Ad1, welke mogelijkheden zijn er om dergelijke documenten veilig te versturen
Uitgangspunt is het digitaal versturen. Er zijn verschillende mogelijkheden om dergelijke documenten beveiligd digitaal te versturen:

1. “Handmatige” encryptie.
   In dit alternatief versleutelt de psycholoog het rapport met een encryptieprogramma, bijvoorbeeld met het gratis en via internet downloadbare 7ZIP en stuurt dat naar de cliënt. Daarbij bestaat het proces uit de volgende stappen:
   - De psycholoog bedenkt een sleutel.
   - De psycholoog versleutelt het rapport met de sleutel in bijvoorbeeld 7ZIP (7ZIP is veelal in enkele seconden klaar)
   - De psycholoog mailt het versleutelde rapport naar de cliënt.
   - De psycholoog verstuurt de sleutel via een ander kanaal naar de cliënt. Bijvoorbeeld dmv SMS of hij belt de cliënt.
   - De cliënt krijgt het rapport via e-mail en de sleutel via SMS. Informatie wordt via verschillende kanalen verstuurd.

   Voordelen:
   - Een veilige methode omdat inhoud en sleutel van elkaar gescheiden zijn (iemand die het bericht onderschept moet ook beschikken over de mobiel van de cliënt om te kunnen beschikken over de sleutel en bovendien moet hij weten dat de sleutel via SMS wordt verzonden)

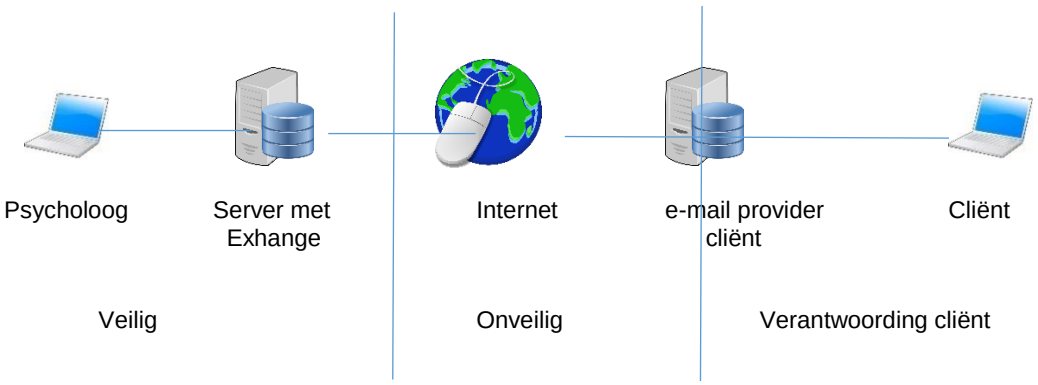
   Nadelen:
   - Het vergt nogal wat manueel werk van zowel de psycholoog als de cliënt
   - Beiden moeten beschikken over 7ZIP en als dat niet het geval is dan moet dat eerst worden gedownload en geïnstalleerd
   - De psycholoog moet wel een “sterke” sleutel bedenken en dat ook administreren voor het geval de cliënt er niet uitkomt, SMS kwijtraakt, enz. Dus een administratie opzetten en ook een mechanisme om sleutels na verloop van tijd te wissen om te voorkomen dat deze gegevens “eeuwig” bewaard blijven.

2. Automatische encryptie
   E-mail in zijn huidige vorm heeft als voordeel het grote gebruikersgemak en de eenvoud van werken. Het nadeel is dat de huidige e-mail protocollen niet voorzien in een veilige verzending doordat een bericht in “plain text” verzonden wordt via het internet.
   Er zijn verschillende manieren om berichten digitaal veilig te versturen waarvoor een organisatie veelal extra producten moet aanschaffen. Die extra producten zorgen er voor dat een bericht wordt versleuteld vanaf de verzender tot aan de ontvanger. Daartoe zijn verschillende oplossingen in de markt. Een niet uitputtende lijst:
   - Zivver
   - Cryptshare
   - File locker

   Het is aan de psycholoog te bepalen welke oplossing voor hem/haar geschikt is, past binnen de infrastructuur en kostentechnisch passend is.

Ad2, heeft de psycholoog voldaan aan de vereisten om maximale vertrouwelijkheid te garanderen?
Het antwoord is nee want de psycholoog heeft het bericht onversleuteld via e-mail verzonden.

Ook het antwoord van de systeembeheerder van de psycholoog is onvoldoende. Weliswaar zijn de maatregelen die getroffen zijn uitstekend maar dat betreft een deel van het berichtenverkeer.



Het berichtenverkeer binnen de organisatie van de psycholoog is zoals de systeembeheerder heeft aangegeven veilig en men heeft maatregelen getroffen om de identiteit van de ander te verifiëren. Dat zijn correcte maatregelen en steeds meer organisaties nemen dergelijke maatregelen. Een systeembeheerder behoort overigens wel te weten dat het verzenden van berichten niet veilig is als er geen aanvullende maatregelen worden getroffen om een bericht te beschermen.

Immers zodra een bericht het internet opgaat is de inhoud te lezen voor een ieder die beschikt over de juiste tools. Met name ook omdat het bericht niet versleuteld is, is de vertrouwelijkheid van e-mail verkeer laag.

Het bericht wordt afgeleverd bij de e-mail provider van de cliënt. Die e-mail provider kan een eigen server-park hebben en/of gebruik maken van oplossingen op het internet (cloud). Vandaar de scheidslijn half op internet. Overigens is het de verantwoordelijkheid van de cliënt en haar e-mail provider dat het verkeer tussen haar en de e-mail provider veilig verloopt. Zodra het bericht bij de cliënt is afgeleverd, is het de verantwoording van de cliënt om er veilig mee om te gaan.
Maar vaak blijft e-mail verkeer (nog een tijd) aanwezig op het internet. Veelal hanteert een e-mail provider nog een bewaartermijn. Het hangt ook af van de diensten die een e-mail provider levert en van instellingen die een iemand kiest bij zijn e-mailprovider.

Het is daarom verstandig alle tussenliggende schakels te beschouwen als “onvertrouwd”. Dat betekent dat de verzender maatregelen treft die ervoor zorgen dat een bericht gedurende transport niet door onbevoegden verwerkt kan worden en een methode daartoe is het versleutelen van het bericht.
Het versleutelen is volgens de huidige technologische inzichten, een afdoende methode. Het versleutelen zelf kan op de handmatige wijze, met één van de voornoemde producten of met elk ander willekeurig product.

Bekendheid met / bewustzijn over het onveilige karakter van e-mail.

Wellicht verzachtend is dat bij veel organisaties en heel veel personen het besef ontbreekt dat e-mail niet veilig is. De overheid, in de medische wereld, binnen het bedrijfsleven, in de politiek en tal van andere sectoren wordt nog heel vaak vertrouwelijke informatie via onveilige e-mail verzonden. E-mail is nu eenmaal reuze makkelijk, alom beschikbaar (op een pc, laptop, tablet of mobiel) en gebruikersvriendelijk. De gemiddelde Nederlander staat niet stil bij de onveiligheid (ook de gemiddelde “Amerikaan” staat hier niet bij stil, getuige het feit dat in Amerika de leden van de Democratische Partij heel veel informatie via e-mail met elkaar uitwisselden).

Pas recentelijk zie je meer en meer het besef ontstaan dat e-mail niet veilig is en niet geschikt om vertrouwelijke informatie te verzenden.”

V 2. Het College is het eens met het advies van de deskundige en neemt dit over.

Van belang in dit verband zijn:

- Artikel 72 van de Beroepscode 2015, dat luidt: *“Psychologen nemen in redelijkheid alle voorzorgen dat er in de schriftelijke, telefonische of elektronische communicatie met de cliënt of met andere betrokkenen geen vertrouwelijke gegevens over de cliënt, zonder diens instemming, ter kennis komen van derden. In een vroeg stadium overleggen psychologen daartoe met de cliënt of met betrokken derden hoe de communicatie het best kan verlopen en hoe deze moet worden vormgegeven om de vertrouwelijkheid met betrekking tot de cliënt te bewaren.”*

- De *Vuistregels beveiliging digitale cliëntendossiers van het NIP*. Deze regels dateren uit 2011.

In Hoofdstuk 10 van de Vuistregels staat hoe vertrouwelijke informatie veilig per e-mail te verzenden. Daarbij wordt de in het advies genoemde handmatige encryptiemethode aangegeven.

V 3. Vaststaat dat verweerder zowel het eerste conceptrapport als de herziene versies als PDF document onversleuteld via e-mail aan klaagster heeft gestuurd.
Anders dan de systeembeheerder van verweerder heeft geconcludeerd (namelijk dat de communicatie per e-mail op een zo veilig mogelijke manier is verlopen), is volgens de deskundige niet voldaan aan het vereiste om maximale vertrouwelijkheid te garanderen.
In zijn reactie d.d. 25 september 2018 op het advies van de deskundige erkent verweerder ook dat het beter was geweest indien hij het rapport versleuteld aan klaagster had verzonden.
Het voorgaande impliceert dat verweerders handelwijze strijdig was met artikel 72 van de Beroepscode 2015, zodat klachtonderdeel 1 gegrond is.

<u>Ad klachtonderdeel 2:</u>

V 4. Het opvragen van klaagsters adresgegevens diende, zoals verweerder heeft aangevoerd, een gerechtvaardigd doel en is niet tuchtrechtelijk verwijtbaar. Met verweerder is het College van oordeel dat het klaagster vrijstond om die gegevens niet te verstrekken of te vragen ze uit de administratie te verwijderen. Dit klachtonderdeel is ongegrond.

Ad klachtonderdeel 3:

V 5. Het College acht het begrijpelijk dat klaagster er moeite mee had om de opdracht in te leveren bij iemand die zij niet kende. Dat aan klaagster niet van tevoren is verteld hoe de gang van zaken was aan het einde van de assessmentdag, namelijk dat het de bedoeling was dat zij haar opdracht inleverde bij de nog in het pand aanwezige persoon, acht het College dan ook niet getuigen van zorgvuldigheid. Het gaat naar het oordeel van het College echter te ver om te concluderen dat deze gang van zaken strijdig was met de Beroepscode. Het College heeft met instemming kennisgenomen van verweerders toezegging kandidaten daarover voortaan beter te zullen informeren.
Dit klachtonderdeel is eveneens ongegrond.

V 6. Het College komt tot de slotsom dat klachtonderdeel 1 gegrond is en dat de klachtonderdelen 2 en 3 ongegrond zijn.

V 7. Ten aanzien van de oplegging van een maatregel overweegt het College het volgende.
Verweerder heeft erkend dat het beter was geweest indien hij het conceptrapport versleuteld had verstuurd aan klaagster. Verweerder heeft verklaard dat zowel deze klacht als de inwerkingtreding van de AVG hebben gezorgd voor nog meer bewustzijn op het gebied van privacy en (elektronische) communicatie, en ertoe hebben geleid dat de werkwijze in zijn praktijk zodanig is aangepast dat dergelijke documenten thans versleuteld worden verzonden.
Verweerder heeft het College verzocht er rekening mee te houden dat de e-mailwisseling met klaagster plaatsvond in november 2017, derhalve vóór de inwerkingtreding van de AVG, in een periode dat het bewustzijn op het gebied van privacy bij velen, inclusief hemzelf, minder groot was dan na de inwerkingtreding van en de voorlichting over de AVG. Verweerder verwijst daarbij ook naar het rapport van de deskundige, waarin dit ook wordt vermeld en waarin staat dat men pas recentelijk meer en meer het besef ziet ontstaan dat e-mail niet veilig is en niet geschikt om vertrouwelijke informatie te verzenden.
Het College heeft hiervoor weliswaar begrip, maar wijst erop dat ook vóór de inwerkingtreding van de AVG reeds regels golden met betrekking tot de in acht te nemen vertrouwelijkheid, zoals bijvoorbeeld de genoemde Vuistregels en artikel 72 van de Beroepscode.
In dit verband heeft het College met instemming geconstateerd dat verweerder in zijn brief van 25 september 2018 heeft gesteld dat hij ertoe is overgegaan om, zoals artikel 72 voorschrijft, meer en beter overleg te plegen met cliënten over de wijze waarop zij met de praktijk willen communiceren.
Gelet op het vorenstaande komt het College tot de conclusie dat kan worden volstaan met gegrondverklaring van onderdeel 1 van de klacht, zonder oplegging van een maatregel.

VI De beslissing

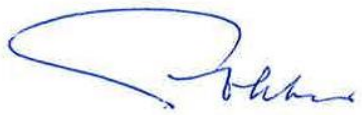
Het College van Toezicht:

- verklaart de klacht deels gegrond als voormeld;
- ziet af van het opleggen van een maatregel.

Aldus gewezen op **20 november 2018** door:

mr. J.P. Fokker, voorzitter,
mr. T.A. Leenhouts-Strijker, secretaris,
mr. drs. M.J. Ariëns,
prof. dr. P.T. Cohen-Kettenis,
prof. dr. M.J.M. van Son,
leden

en ondertekend door de voorzitter,



J.P. Fokker