COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag **BEZOEKADRES** Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 **FAX** 070 - 88 88 501 **INTERNET** www.cbpweb.nl

College bescherming persoonsgegevens

Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V.

z2012-00288

Openbare versie
Rapport definitieve bevindingen

December 2014

INHOUDSOPGAVE

1 INLEIDING

Aanleiding onderzoek

In een televisie-uitzending van ZEMBLA op 20 april 2012 kwam naar voren dat in de software van het computerprogramma Humannet Starter sprake zou zijn geweest van een datalek. Naar aanleiding van deze berichtgeving heeft het College bescherming persoonsgegevens (CBP) bij brief van 20 april 2012 inlichtingen gevraagd bij VCD Humannet B.V. (VCD).

VCD Humannet B.V. is een onderdeel van de VCD IT Groep, een ICT bedrijf dat zowel consultancy, software, infrastructuur en beheer levert. Het beveiligingslek betrof de applicatie Humannet Starter, één van de twee verzuimapplicaties van Humannet waarin arbodiensten en werkgevers medische gegevens van werknemers verwerken. De andere applicatie is Humannet Verzuim. In de applicaties Humannet Starter en Humannet Verzuim werden ten tijde van het beveiligingslek gegevens over de gezondheid van ca. [aantal] werknemers[1] verwerkt.[2]

Ingevolge artikel 13 van de Wet bescherming persoonsgegevens (Wbp) dient een verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

Op grond van de door VCD verstrekte informatie, bij brief van 27 april 2012 en 16 mei 2012 concludeerde het CBP in de brief van 5 juni 2012 aan VCD dat VCD naar aanleiding van het incident beveiligingsmaatregelen had getroffen. Zo had VCD aangegeven dat zij een [soort] token als authenticatie toe zou gaan passen voor alle relaties van VCD, uiterlijk augustus 2012. Ook gaf VCD aan dat zij op korte termijn een security audit zou laten uitvoeren voor Humannet Starter en Humannet Verzuim en deze audits jaarlijks zou herhalen.

Gelet op deze maatregelen zag het CBP op dat moment geen aanleiding meer tot het doen van verder onderzoek naar het datalek. Het CBP verzocht VCD na afloop van de audits nadere informatie aan het CBP te doen toekomen.

Uit de nadere opgevraagde[3] en ontvangen[4] informatie leidde het CBP af dat er aanwijzingen zijn dat VCD onvoldoende maatregelen heeft getroffen om de beveiliging van Humannet Starter en Humannet Verzuim in overeenstemming te brengen met het bepaalde in artikel 13 Wbp.

---

[1] [aantal]in Humannet Starter en [aantal] in Humannet Verzuim. Brief van 11 september 2014 van VCD aan het CBP.

[2] In de brief van 11 september 2014 van VCD aan het CBP is aangegeven dat dit aantal inmiddels is gedaald naar [aantal] medewerkers.

[3] Telefonisch op 11 november 2012, 5 februari 2013, 4 april 2013, 11 april 2013 en 15 april 2013. Bij brieven van het CBP aan VCD van 28 februari 2013, 28 maart 2013, 23 april 2013, 3 juni 2013, 3 december 2013, 17 december 2013.
Bij e-mail van het CBP aan VCD van 4 april 2013.

[4] Telefonisch op 11 november 2012, 5 februari 2013, 4 april 2013, 11 april 2013, 15 april 2013. Bij brieven van VCD aan het CBP van 13 februari 2013, 8 maart 2013, 15 maart 2013, 13 juni 2013 en 11 juli 2013. Bij e-mails van VCD aan het CBP van 4 april 2013, 11 april 2013, 12 april 2013, 16 april 2013, 18 april 2013 en 25 april 2013.

Het CBP heeft daarom een ambtshalve onderzoek ingesteld naar de beveiliging van de (medische) persoonsgegevens in Humannet Verzuim en Humannet Starter. Dit is bij brief van 8 augustus 2013 aan VCD kenbaar gemaakt.

Doel van het onderzoek

Het doel van het onderzoek is te onderzoeken of VCD voldoende passende technische en organisatorische maatregelen ten uitvoer brengt om de (medische) persoonsgegevens in Humannet Starter en Humannet Verzuim te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking als bedoeld in artikel 13 Wbp. Het onderzoek richt zicht hierbij specifiek op de volgende vragen:

- Is meerfactor authenticatie ingevoerd voor alle gebruikers die toegang hebben tot medische gegevens in Humannet Starter en Humannet Verzuim?
- Worden in de applicaties Humannet Starter en Humannet Verzuim technische risico's geïdentificeerd middels het periodiek uitvoeren van penetratietesten/ security scans door VCD en/ of een externe partij?
- Worden passende organisatorische en/ of technische maatregelen getroffen om de risico's in de systemen Humannet Starter en Humannet Verzuim te beperken danwel te voorkomen?

Verloop onderzoek datalek

Bij brief van 20 april 2012 heeft het CBP een inlichtingenverzoek uitgezet bij VCD. Bij brief van 27 april 2012 heeft VCD inlichtingen verstrekt.

Bij brief van 10 mei 2012 heeft het CBP aanvullende vragen gesteld aan VCD. Deze zijn bij brief van 16 mei 2012 beantwoord.

Bij brief van 5 juni 2012 heeft het CBP aangegeven op dat moment af te zien van verder onderzoek.

Telefonisch heeft het CBP op 11 september 2012 contact gezocht met VCD over de datum van aanlevering van de security audits en nadere vragen over de authenticatie, die niet ingevoerd bleek te zijn op de door VCD gestelde datum.

Op 7 februari 2013 heeft het CBP nogmaals contact opgenomen met VCD met het verzoek om de security audits aan te leveren en schriftelijk informatie aan het CBP te doen toekomen over de authenticatie.
Bij brief van 13 februari 2013 heeft VCD hierop gereageerd.

Bij brief van 28 februari 2013 heeft het CBP de security audits van Humannet Starter en Humannet Verzuim gevorderd bij VCD en meer informatie opgevraagd over de authenticatie.
Bij brief van 8 maart 2013 heeft VCD op de vordering gereageerd, maar de opgevraagde documenten niet meegestuurd.
Het CBP heeft telefonisch contact opgenomen met VCD op 11 en 15 maart 2014.
Bij brief van 15 maart 2013 heeft VCD de security-audit (heronderzoek) van Humannet Verzuim van 21 december 2012 en de security-audit (technische beveiligingsonderzoek) van Humannet Starter van 27 juli 2012 aan het CBP doen toekomen.

Bij brief van 28 maart 2013 heeft het CBP nogmaals alle security audits gevorderd omdat het heronderzoek van Humannet Starter en het technische beveiligingsonderzoek van Humannet Verzuim ontbraken. Tevens heeft het CBP een lijst met gegevens van klanten van Humannet Starter en Humannet Verzuim gevorderd.

Telefonisch is op 4 april 2013 contact geweest tussen de advocaat van VCD en het CBP en heeft VCD aangegeven geen heronderzoek van Humannet Starter te hebben. De concept-audit (technisch beveiligingsonderzoek) van Humannet Verzuim van 22 juni 2012 is door VCD aan het CBP geleverd.

Bij brief van 12 april 2013 heeft VCD laten weten de lijst met klantgegevens en de planning van de invoering van meerfactor authenticatie niet te willen verstrekken. Op 15 april is hierover telefonisch contact geweest tussen het CBP en de advocaat van VCD.

Bij brief van 16 april 2013 is door VCD aangegeven dat zij de lijst met klantgegevens niet aan het CBP verstrekt.
Bij brief van 18 april 2013 heeft VCD een planning van de invoering van meerfactor authenticatie aan het CBP doen toekomen.
Bij brief van 23 april 2013 heeft het CBP een rappel vordering voor de lijst met klantgegevens aan VCD verstuurd.
Bij brief van 25 april 2013 heeft VCD nogmaals geweigerd de gevraagde gegevens te versturen.

Bij brief van 3 juni 2013 is een last onder dwangsom opgelegd aan VCD waarin VCD is gesommeerd de lijst met klantgegevens te verstrekken.
Op 4 juni 2013 heeft VCD telefonisch contact opgenomen met het CBP met het verzoek voor een gesprek tussen de voorzitter van het CBP en de algemeen directeur van de VCD IT-groep). Het CBP heeft aangegeven hieraan geen gevolg te geven.
Bij brief van 13 juni 2013 van VCD is de gevraagde lijst met klantgegevens verstrekt.

Bij brief van 11 juli 2013 heeft VCD het CBP laten weten dat zij het ISO 27001-certificaat heeft behaald.

Verloop onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim

Het CBP heeft VCD bij brief van 8 augustus 2013 geïnformeerd dat een ambtshalve onderzoek is gestart naar de beveiliging van de verzuimapplicaties Humannet Starter en Humannet Verzuim.

Bij brief van 30 november 2013 heeft VCD een update gegeven over de beveiligingsmaatregelen die zij heeft getroffen.
In het kader van het ambtshalve onderzoek heeft het CBP bij brieven van 3 december 2013 en 17 december 2013 inlichtingen gevraagd aan VCD.
VCD heeft inlichtingen verstrekt bij brieven van 6 december 2013 en 15 januari 2014 en bij e-mail van 28 april 2014.
Bij brief van 26 mei 2014 heeft het CBP inlichtingen gevorderd bij VCD Humannet. Bij e-mail van 4 juni 2014 heeft VCD uitstel verzocht tot en met week 27. Bij brief van 5 juni 2014 heeft het CBP uitstel verleend tot 17 juni 2014. Bij brief (per e-mail) van 17 juni 2014 en poststuk van 18 juni 2014 heeft VCD de gevorderde inlichtingen verstrekt.

Bij brief van 7 augustus 2014 heeft het CBP het rapport voorlopige bevindingen aan VCD doen toekomen.
Bij brief van 5 september 2014 heeft VCD in aansluiting op de brief van 17 juni 2014 de resultaten van penetratietesten in de periode 12 mei t/ m 27 augustus 2014 (Humannet Starter) en 9 juni t/ m 7 juli 2014 (Humannet Verzuim) aan het CBP verzonden.
Bij brief van 11 september 2014 heeft VCD een zienswijze gegeven op het rapport voorlopige bevindingen.
Bij brief van 3 oktober 2014 heeft VCD nadere informatie aan het CBP doen toekomen over de brief die zij aan klanten heeft gestuurd met de aankondiging van meervoudige authenticatie bij toegang tot medische gegevens.
Telefonisch op 21 oktober 2014 heeft het CBP contact opgenomen met de advocaat van VCD over een zinsnede in de zienswijze van 11 november 2014.
Bij e-mail van 21 oktober 2014 heeft de advocaat van VCD verduidelijking gegevens.
Bij e-mails van 7 november 2014, 10 november 2014 en 14 november 2014 heeft het CBP nadere informatie opgevraagd bij VCD over de applicaties Humannet Starter en Humannet Verzuim.
Bij e-mails van 12 november 2014 en 17 november 2014 heeft VCD de gevraagde informatie verstrekt.

Onderzoek bij klanten van VCD
In het kader van het onderzoek naar de beveiliging van de verzuimapplicaties Humannet Starter en Humannet Verzuim, zijn tevens inlichtingen gevraagd bij enkele klanten van Humannet Verzuim en Humannet Starter.

Bij brief van 30 september 2013 heeft het CBP inlichtingen gevraagd bij klant 1 over de beveiliging van Humannet Starter.
Bij brieven van 10 november en 24 november 2013 heeft klant 1 de gevraagde inlichtingen verstrekt.
Bij brief van 16 december 2013 heeft het CBP het onderzoek bij klant 1 beëindigd omdat klant 1 de samenwerking met VCD heeft beëindigd.

Bij brief van 30 september 2013 heeft het CBP inlichtingen gevraagd bij klant 2 over de beveiliging van Humannet Starter.
Bij brieven van half oktober 2013 en 31 oktober 2013 heeft klant 2 de gevraagde inlichtingen verstrekt.
Bij brief van 16 december 2013 heeft het CBP het onderzoek bij klant 2 beëindigd omdat klant 2 aangaf de samenwerking met VCD op korte termijn te beëindigen.

Bij brieven van 17 december 2013 en 14 februari 2014 en telefonisch op 25 en 29 april 2014 heeft het CBP inlichtingen gevraagd bij klant 3 over de beveiliging van Humannet Starter.
Bij brieven van 13 januari 2014, 1 april 2014 en 2 juli 2014 en e-mail van 28 en 29 april 2014 heeft klant 3 de gevraagde inlichtingen verstrekt.
Bij e-mail van 15 augustus 2014 heeft klant 3 bevestigd dat meervoudige authenticatie in week 29 (14 t/ m 18 juli) 2014 voor alle medewerkers is ingevoerd.
Bij brief van 20 augustus 2014 heeft het CBP het onderzoek bij klant 3 beëindigd.

2 JURIDISCH KADER

Verwerking van persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*.

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp als "*elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.*"

Verantwoordelijke

Op grond van artikel 1, aanhef en onder d, van de Wbp is de verantwoordelijke *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*.

De wetsgeschiedenis geeft hierover aan: "*Het begrip 'verantwoordelijke' knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden. De richtlijn gaat ervan uit dat deze bevoegdheden in de regel in dezelfde hand liggen. Is dit niet het geval, dan is er sprake van gezamenlijke verantwoordelijkheid. [...]*
Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele inhoud van het begrip."[5]

Bewerker

Op grond van artikel 1, aanhef en onder e, van de Wbp is de bewerker *degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderwerpen*.

In de memorie van toelichting staat over de bewerker: "*Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz.'*[6]

Ook staat in de memorie van toelichting over de bewerker: "*Hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking door de bewerker (zie artikel 12), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens (hoofdstuk 1 en 2 van dit wetsvoorstel).*[7]

[5] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 55.
[6] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 61.
[7] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 61.

Behoorlijke en zorgvuldige gegevensverwerking

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt.

"*De wetsgeschiedenis geeft aan dat het woord 'wet' mede betrekking heeft op andere wetgeving inzake de verwerking van persoonsgegevens. Het gaat hier dus om een schakelbepaling die verzekert dat de betrokken regelingen in onderling verband van toepassing zijn*."[8] Dit betekent (onder meer) dat een overtreding van artikel 13 Wbp eveneens leidt tot een overtreding van de algemene norm vervat in artikel 6 Wbp.

Beveiliging

Ingevolge artikel 13 van de Wbp dient een verantwoordelijke *passende technische en organisatorische maatregelen ten uitvoer te brengen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te bescherming gegevens met zich meebrengen.*

In het begrip "passende" ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Daarnaast duidt het begrip "passende" op een proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van deze gegevens.[9] Medische gegevens behoren tot de categorie bijzondere gegevens als bedoeld in artikel 16 Wbp. Dit betekent dat hoge eisen gesteld worden aan de technische en organisatorische maatregelen ter bescherming van deze gegevens.

Passende maatregelen

Om vast te stellen wat passende maatregelen zijn, zoals bedoeld in artikel 13 Wbp, gebruikt het CBP de richtsnoeren 'Beveiliging van persoonsgegevens'[10] in samenhang met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging[11] en de ICT-Beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum[12]. Ook invulling van open normen door het Forum Standaardisatie en het College Standaardisatie[13] worden door het CBP gebruikt om vast te stellen wat passende maatregelen zijn, zoals in dit onderzoek het document 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten'[14] .

[8] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 78.
[9] Kamerstukken II, 1997/ 98, 25 892, nr. 3, p. 98-99.
[10] CBP Richtsnoeren beveiliging van persoonsgegevens, februari 2013.
[11] NEN-ISO/ IEC 27002 2007 nl.
[12] ICT-Beveiligingsrichtlijnen voor webapplicaties, deel 1, januari 2012, deel 2, januari 2012.
[13] College en Forum Standaardisatie zijn in 2006 ingesteld door het kabinet. Beide instellingen bevorderen digitale samenwerking (interoperabiliteit) tussen overheden onderling en tussen overheid, bedrijven en burgers. Dit zorgt ervoor dat verschillende digitale systemen steeds beter op elkaar zullen aansluiten, en dat gegevens makkelijker te delen zijn. Het gebruik van open standaarden speelt hierbij een belangrijke rol. Zie ook: www.forumstandaardisatie.nl.
[14] Een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2013.

In de volgende paragrafen zet het CBP uiteen wat passende maatregelen zijn ten aanzien van:

- de authenticatie bij toegang tot een bestand met medische persoonsgegevens;
- de identificatie van technische kwetsbaarheden in een applicatie waarin medische persoonsgegevens worden verwerkt en het zoveel mogelijk beperken van veiligheidsrisico's door (geconstateerde) kwetsbaarheden.

Passende maatregelen ten aanzien van authenticatie

Authenticatie is het proces waarbij wordt nagegaan of een gebruiker die in wil loggen in een applicatie/ systeem daadwerkelijk is wie hij/ zij beweert te zijn. Het invoeren van een gebruikersnaam en wachtwoord is een voorbeeld van authenticatie middels één factor, namelijk het wachtwoord. Het invoeren van een gebruikersnaam, password en een sms-code is een voorbeeld van twee factor authenticatie.

In de ICT-Beveiligingsrichtlijnen voor webapplicaties van het NCSC[15] staat de volgende beveiligingsrichtlijn ten aanzien van toegangsbeveiliging:
"*B0-12 Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/ toegangsbeheer.*

- *Voorkom ongeautoriseerde toegang tot netwerken, besturingssystemen, informatie en informatiesystemen en –diensten, zodat schade bij misbruik zo beperkt mogelijk is.*"

In de Code voor Informatiebeveiliging staat "*Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.*"[16]
en
"*Waar krachtige authenticatie en verificatie van de identiteit nodig zijn, behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals cryptografische hulpmiddelen, smartcards, 'tokens' of biometrische hulpmiddelen. De sterkte van de gebruikersidentificatie en authenticatie behoort geschikt te zijn voor de gevoeligheid van de informatie waartoe toegang wordt verleend.*"[17]

De NEN-7510, die aanwijzingen geeft voor het toepassen van de Code voor informatiebeveiliging ISO/ IEC 27002 in de gezondheidszorg, stelt de volgende eis:
"*Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken.*"[18].

In 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten'[19] worden de verschillende niveaus van authenticatie uitgewerkt. Hierin wordt gesteld dat de verwerking van medische gegevens een verwerking van persoonsgegevens in risicoklasse III betreft. Hiervoor is tenminste een betrouwbaarheidsniveau 3 vereist.[20] Volgens het STORK-raamwerk[21] vereist dit niveau "*striktere methoden voor de verificatie van de geclaimde identiteit van de gebruiker. Deze moeten een hoge mate van zekerheid bieden. […] Als type middel is 2-factor authenticatie vereist; gedacht kan worden aan 'soft' certificaten of one-time-passwords tokens.*"

---

[15] Deel 1, januari 2012, pag. 17..
[16] NEN-ISO/ IEC 27002:2007 nl, pag. 76.
[17] NEN-ISO/ IEC 27002:2007 nl, pag. 80.
[18] NEN-7510 (2011), p. 98.
[19] Een handreiking voor overheidsorganisaties, Forum Standaardisatie, augustus 2013.
[20] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, pag 22 en pag. 27.
[21] Dit raamwerk is in EU-verband ontwikkeld en vormt de 'ruggengraat' van het stelsel van betrouwbaarheidsniveaus waaraan enerzijds (families van) overheidsdiensten en anderzijds de beschikbare authenticatiemiddelen gekoppeld kunnen worden. Zie www.eid-stork.eu.

Uit de bovengenoemde beveiligingsstandaarden vloeit voort dat ten aanzien van authenticatie bij de toegang tot applicaties die specifiek zijn gericht op het verwerken van medische gegevens en waarbij toegang wordt verschaft via het internet, tenminste gebruik dient te worden gemaakt van tweefactor authenticatie.

Passende maatregelen ten aanzien van technische kwetsbaarheden
In de CBP richtsnoeren ´beveiliging van persoonsgegevens´ is aangegeven dat artikel 13 Wbp bij de beveiliging van persoonsgegevens een risicogerichte benadering vergt. "*De verantwoordelijke inventariseert de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die dit incident kan hebben en de kans dat deze gevolgen zich voordoen. […] Bij verwerking via internet is bijvoorbeeld hacking een dreiging waarmee rekening moet worden gehouden […] De verantwoordelijke treft maatregelen op basis van de uitgevoerde risicoanalyse en kiest de maatregelen zodanig dat wordt voldaan aan de vastgestelde betrouwbaarheidseisen*." [22]

In de Code voor Informatiebeveiliging staat: "*Er behoren passende en tijdige handelingen te worden genomen als reactie op identificatie van mogelijke technische kwetsbaarheden*."[23]
De norm NEN 7510, die aanwijzingen geeft voor het toepassen van de Code voor informatiebeveiliging ISO/ IEC 27002 in de gezondheidszorg, stelt: "*Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.*"[24]

In de ICT-Beveiligingsrichtlijnen voor webapplicaties van het NCSC[25] staan onder andere de volgende algemene beveiligingsrichtlijnen:
B0-2 Voer actief risicomanagement uit.

- *Het bewust komen tot betrouwbaarheidseisen en maatregelen aan de hand van een methodische beoordeling van beveiligingsrisico's.*
- *Het periodiek evalueren van de beveiligingsrisico's en geïmplementeerde maatregelen.*

B0-8 Penetratietests worden periodiek uitgevoerd.

- *Inzicht krijgen en houden in de mate waarin een webapplicatie weerstand kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken webapplicatie).*

B0-9 Vulnerability assessments (security scans) worden periodiek uitgevoerd.

- *Inzicht hebben in de mate waarin de ICT-omgeving bekende kwetsbaarheden en zwakheden bevat, zodat deze waar mogelijk weggenomen kunnen worden.*"

Uit de bovengenoemde beveiligingsstandaarden vloeit voort dat ten aanzien van technische kwetsbaarheden tenminste aan de volgende vereisten dient te worden voldaan:

- beveiligingsrisico's dienen periodiek in kaart worden gebracht, bijvoorbeeld middels penetratietesten en/ of security scans;
- er moeten passende (organisatorische en/ of technische) maatregelen worden getroffen om risico's te beperken danwel te voorkomen.

[22] CBP Richtsnoeren beveiliging van persoonsgegevens, pag. 15.
[23] NEN-ISO/ IEC 27002:2007 nl, paragraaf 12.6.
[24] NEN 7510:2011nl, paragraaf 12.6.1.
[25] Deel 1, januari 2012, pag. 17..

3 FEITEN VOORLOPIGE BEVINDINGEN

In dit hoofdstuk worden de feiten besproken zoals die in het onderzoek voorafgaand aan de voorlopige bevindingen zijn geconstateerd. In hoofdstuk 4 volgt de integrale tekst van de beoordeling van deze feiten in het rapport voorlopige bevindingen. Nadat VCD de voorlopige bevindingen heeft ontvangen heeft zij haar zienswijze gegeven op de beoordeling in de voorlopige bevindingen en enkele nieuwe feiten aangedragen. De zienswijze en de nieuwe feiten worden in hoofdstuk 5 besproken. Hoofdstuk 6 bevat de definitieve beoordeling.

Verwerking van persoonsgegevens

In de applicaties Humannet Starter en Humannet Verzuim worden gegevens verwerkt van [aantal][26] actieve medewerkers.[27] Het betreft tenminste de volgende gegevens:

- Medewerker (Naam, Geslacht, Geboortedatum, Geboortenaam en Partner).
- Adres (Adres, Postcode en Woonplaats).
- Nummer (Telefoon, Mobiel, Fax en E-mail).
- Functiegegevens (Intern medewerker nummer, Functie, BSN, Datum in dienst, Datum uit dienst, Dienstverband en Afdelingsnummer).
- Werkpatroon (Normuren per week , Uren per dag, FTE, Type dienstverband).
- Salaris (Bruto salaris, Periode salarisuitbetaling, Bankgegevens).
- Arbeidshandicap (Categorie, einddatum beschikking).
- Medische en verzuimdossiers (Algemeen, Eigen werk, Medisch beeld, Onderzoek, Privesituatie, Copingstijl, Diagnose, Beperkingen, Prognose eigen werk, Prognose aangepast werk, Cas-code, CVO-code, Arbeid gerelateerd, Beroepsziekte, Mededeling voor verzuimmanager, Mededeling voor werkgever.

De werkwijze van VCD

VCD geeft aan [aantal] klanten te hebben die gebruik maken van Humannet Starter of Humannet Verzuim.[28]
De klanten van VCD (arbodiensten en werkgevers) gebruiken Humannet Starter en Humannet Verzuim bij de verzuimbegeleiding van (zieke) werknemers. De klanten registreren de bovengenoemde gegevens van de werknemers in de applicatie Humannet Starter of Humannet Verzuim.

Op de website van VCD[29] staat:
"*Met onze verzuimsoftware geeft u uw verzuimbeleid perfect vorm. Samen met u stellen wij het ideale verzuimsysteem samen. Een verzuimsysteem dat perfect aansluit bij de processen binnen uw organisatie en rekening houdt met uw eisen en wensen.*
[…]
Met onze slimme verzuimsoftware houdt u op een snelle en efficiënte manier uw verzuimdossiers bij. Zo kunt u de protocollen aanpassen per bedrijfstak (cao), per organisatie of zelfs per afdeling. Onze software leidt u op intelligente wijze stap voor stap door het protocol in al zijn episodes en contactmomenten. U krijgt voortdurend haarscherp in beeld wat moet worden ingevoerd. Historie, voortgang, status, acties, vervolgtraject: niets ontgaat u."
[…]

---

[26] [aantal] in Humannet Starter en [aantal] in Humannet Verzuim.
[27] Brief van 27 april 2013 van VCD aan het CBP en e-mail van 28 april 2014 van VCD aan het CBP.
[28] Bij brief van 6 december 2013 heeft het CBP van VCD een lijst met klanten ontvangen, waarin [aantal] klanten staan vermeld.
[29] http:/ / www.vcdhumannet.nl/ verzuimsoftware, 12 mei 2014.

Onze verzuimsoftware is zeer flexibel in te richten. Het gaat uit van de processen binnen uw organisatie en niet andersom. Onze medewerkers staan voor u klaar om u te ondersteunen bij de inrichting van de software. Ze kennen uw markt en weten dus precies wat u nodig heeft."

VCD stelt in de brief van 13 april 2013 aan het CBP: "*Het is van belang op te merken dat VCD Humannet geen medische en persoonlijke gegevens verwerkt. Zij stelt de applicatie Humannet Starter ter beschikking, doch verwerkt zelf geen gegevens.*"

In de brief van 6 juni 2013 van VCD aan de relaties[30] staat onder andere: "*De verantwoordelijke dient op grond van de Wbp passende technische en organisatorische maatregelen te treffen om het verlies van gegevens of onrechtmatig verwerken tegen te gaan. Deze maatregelen moeten een passend beschermingsniveau garanderen. Wanneer u hiervoor een leverancier van een verzuimsysteem (een 'bewerker') inschakelt, moet u ervoor zorgen dat deze eveneens passende beveiligingsmaatregelen neemt.*
U zult soms niet zelf al uw persoonsgegevens verwerken, maar de feitelijke handelingen geheel of gedeeltelijk laten verrichten door een daarin gespecialiseerde organisatie zoals VCD Humannet. Ook degene die ten behoeve van de verantwoordelijke gegevens verwerkt is 'bewerker'. De Wbp stelt eisen aan de vorm en inhoud van de afspraken die u met een bewerker, in dit geval VCD Humannet maakt, en eist dat deze schriftelijk vastgelegd worden: […]".

In de brief van 30 november 2013 van VCD aan het CBP stelt VCD: "*De Wbp stelt eisen aan de vorm en de inhoud van de afspraken die een verantwoordelijke met een bewerker, in dit geval VCD Humannet, maakt en eist dat deze schriftelijk vastgelegd worden. Op 6 juni 2013 hebben wij aan onze relaties een brief gezonden (zie bijlage 4) waarin de werking van de Wbp en de termen 'verantwoordelijke' en 'bewerker' zijn toegelicht. Bijgevoegd hebben wij een bewerkersovereenkomst waarin alle door de Wbp opgelegde verplichtingen met betrekking tot het verwerken van persoonsgegevens zijn opgenomen (zie bijlage 5). Door het ondertekenen van deze overeenkomst heeft onze klant als verantwoordelijke en als relatie van VCD Humannet alles goed geregeld.*"

Tijdens het onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim zijn zowel inlichtingen gevraagd aan VCD als aan drie klanten van VCD.[31]

Het CBP heeft onder andere gevraagd waar de applicatie draait.
In de antwoorden van de klanten die gebruik maken van Humannet is hierover aangegeven:

- "*De applicatie draait bij de leverancier (VCD).*"[32]
- "*De applicatie staat niet op een server in de IT omgeving van [klant 3] geïnstalleerd. De applicaties van VCD Humannet draaien in een omgeving bij VCD.*"[33]
- "*De Humannet Starter applicatie en de databases met (i) basisgegevens en verzuimregistraties en (ii) medische gegevens zijn geïnstalleerd op verschillende servers die ten behoeve van VCD Humannet worden gehost door* […]."[34]

[30] De gebruikers van de applicaties.
[31] Het CBP heeft in het kader van het onderzoek naar Humannet ook onderzoek uitgevoerd bij 3 klanten van VCD. Eén van de klanten heeft tijdens het onderzoek de samenwerking met VCD beëindigd, één klant heeft aangegeven over te gaan op een ander systeem, en bij de derde klant loopt het onderzoek van het CBP nog.
[32] Brief van 31 oktober 2013 van klant 2 aan het CBP, antwoord op vraag 5.
[33] Brief van 13 januari 2013 van klant 3 aan het CBP, antwoord op vraag 5.
[34] Brief van 10 november 2013 van de advocaat van klant 1 aan het CBP, antwoord op vraag 5.

Ook heeft het CBP gevraagd wie de applicatie beheert. Hierop antwoorden de klanten het volgende.

- "*De applicatie wordt beheerd door de leverancier*".[35]
- "*Beheer van de applicatie berust bij VCD Humannet* […]."[36]
- "*VCD Humannet voert het operationeel en technisch beheer uit* […]."[37]

Op de vraag of personen van VCD Humannet toegang hebben tot de persoonsgegevens die de klanten in de applicatie verwerken antwoorden de klanten het volgende.

- "*Een beperkt aantal medewerkers van VCD Humannet heeft toegang tot (persoons)gegevens van [klant 2].* […]."[38]
- "*Ja, VCD Humannet heeft toegang tot de gegevens die [klant 3] in de verzuimapplicatie verwerkt.*"[39]
- "*Op basis van de overeenkomst tussen [klant 1] en VCD Humannet, heeft een beperkt aantal medewerkers van VCD Humannet en VCD Infra Solutions toegang toe de Humannet Starter omgeving en dus de (persoons)gegevens die in de applicatie worden verwerkt.* […]"[40]

Beveiliging

Authenticatie

In de brief van 16 mei 2012 aan het CBP stelt VCD dat zij een [soort] token als authenticatie toe gaat passen voor alle relaties van VCD, uiterlijk augustus 2012.

Op 11 september 2012 geeft VCD aan[41] dat de planning wat uitloopt maar dat het eind oktober 2012 rond is dát ze het gaan doen. Daarna wordt het ingevoerd. VCD zal contact opnemen met het CBP als de implementatie van start gaat.

Op 7 februari 2013 geeft VCD aan[42] dat de meerfactor authenticatie nog niet is ingevoerd. In het telefoongesprek geeft VCD aan dat zij met een pilot gaat starten.

In de brief van 13 februari 2013 van VCD aan het CBP stelt VCD: "*[…] Doel is om op korte termijn een POC (proof of concept) te starten […] Verwachting is dat de doorlooptijd van de POC ongeveer 3 a 4 maanden is.*"

Bij e-mail van 18 april 2013 van de advocaat van VCD heeft het CBP de gevorderde planning[43] ontvangen waarin staat dat de livegang van de sterke authenticatie op 22 november 2013 zal plaatsvinden.

Bij brief van 6 juni 2013 van VCD aan de gebruikers van de applicaties stelt VCD: "*In de afgelopen periode hebben wij u geïnformeerd dat VCD Humannet gekozen heeft voor het Authenticatieplatform van [Naam bedrijf]. De verwachting is dat medio november dit jaar sterke authenticatie volledig is toegepast in onze producten*."

[35] Brief van 31 oktober 2013 van klant 2 aan het CBP, antwoord op vraag 6.
[36] Brief van 13 januari 2013 van klant 3 aan het CBP, antwoord op vraag 6.
[37] Brief van 10 november 2013 van de advocaat van klant 1 aan het CBP, antwoord op vraag 6.
[38] Brief van 31 oktober 2013 van klant 2 aan het CBP, antwoord op vraag 9.
[39] Brief van 13 januari 2013 van klant 3 aan het CBP, antwoord op vraag 9.
[40] Brief van 10 november 2013 van de advocaat van klant 1 aan het CBP, antwoord op vraag 9.
[41] Telefoongesprek van het CBP met VCD op 11 september 2012
[42] Telefoongesprek van het CBP met VCD op 7 februari 2013.
[43] Gevorderd door het CBP bij brief van 28 maart 2013.

In de brief van 30 november 2013 van VCD aan het CBP stelt VCD: "*De huidige stand van zaken is dat we op 22 november gereed zullen zijn om onze klanten met sterke authenticatie uit te rusten*."

In de brief van 13 januari 2014 van klant 3 aan het CBP geeft zij aan dat klant 3 nog geen gebruik maakt van sterke(re) authenticatie, "echter hebben wij wel sterk aangedrongen bij VCD Humannet om dit te implementeren."
Klant 3 geeft aan dat deze authenticatie eind kwartaal 1 van 2014 geïmplementeerd zal zijn.

Bij brief van 1 april 2014 van Klant 3 aan het CBP stelt Klant 3: "*Graag willen wij terugkomen op het feit dat wij gestreefd hebben om voor d.d. 31 maart 2014 de sterke authenticatie ingeregeld te hebben. Inmiddels is alles geformaliseerd maar neemt de implementatie iets meer tijd in beslag dan wij vooraf hadden verwacht. Wij gaan ervan uit om zo snel mogelijk, doch uiterlijk 1 juni aanstaande, de sterke authenticatie geïmplementeerd te hebben binnen [klant 3].*"

In de brief van 15 januari 2014 van VCD aan het CBP is een klantenlijst toegevoegd waarin van [aantal] klanten is aangegeven of ze wel of niet hebben aangegeven sterke authenticatie te willen gaan toepassen.
Van deze [aantal] klanten hebben [aantal] klanten (waaronder klant 3) aangegeven het te willen gaan toepassen, [aantal] heeft aangegeven geen interesse te hebben en van de overige klanten is geen reactie ontvangen.

In de brief van 17 juni 2014 stelt VCD: "*Ten aanzien van onze klanten hebben wij ze allemaal aangeschreven met de mogelijkheid tot het afnemen van sterke authenticatie. Dit leidde tot [aantal] offerteaanvragen, die zijn uitgemond in [aantal] getekende offertes, waarbij voor [aantal] de implementatie in volle gang is*."

In de brief van 2 juli 2014 van klant 3 is door klant 3 aangegeven dat de implementatie niet gereed was op 1 juni 2014, omdat "*een aantal technische problemen zijn geconstateerd, waardoor de meervoudige authenticatie niet voor alle gebruikers toegankelijk was*".
Klant 3 geeft aan dat zij verwacht dat de implementatie de komende maand zal worden afgerond.

Technische kwetsbaarheden

In de brief van 27 april 2012 van VCD aan het CBP heeft VCD aangegeven dat er elk jaar zowel voor Humannet Starter als voor Humannet Verzuim een uitgebreide audit (Black Box/ Grey Box) zal worden uitgevoerd.

Het CBP heeft in het onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim 3 audits ontvangen. Het betreft de volgende audits:

- [Naam bedrijf, naam rapport], versie 1.0, 27 juli 2012.
- [Naam bedrijf, naam rapport], versie 0.2, 22 juni 2012.
- [Naam bedrijf, naam rapport], versie 0.2, 21 december 2012.[44]

[44] Het CBP heeft tevens ontvangen de audit [Naam bedrijf, naam rapport], definitief versie 1.0, 25 februari 2013'. Zoals blijkt uit het documentbeheer in het rapport (pag iii) is dit een definitieve versie van het rapport dat op 20-12-2012 is opgesteld en op 21-12-2012 intern is gereviewd.

In deze audits worden conclusies getrokken ten aanzien van de beveiliging van Humannet Starter en Humannet Verzuim.
[Naam bedrijf] maakt het volgende voorbehoud in haar rapportages over de beoordeling op basis van de resultaten: "*Omdat de uiteindelijke business impact door ons nauwelijks is in te schatten, dienen de bevindingen en hun beoordelingen door VCD geïnterpreteerd te worden in de context van het systeem*."[45]

Humannet Starter
Ten aanzien van de beveiliging van Humannet Starter wordt in de audit[46] van Humannet Starter geconcludeerd:

- 27 juli 2012: de beveiliging van Humannet Starter is '*zeer onveilig*'. In de audit staat: " *Doordat we een aantal kwetsbaarheden hebben gevonden waarvan uitbuiting grote gevolgen kan hebben, beoordelen we de applicatie als zeer onveilig*".[47]
  Uit de audit[48] blijkt dat er 5 hoge risico's zijn aangetroffen:
  - [risico];
  - [risico];
  - [risico];
  - [risico] en
  - [risico].

  Voorts zijn er in de audit 6 gemiddelde risico's aangetroffen, 25 lage risico's en 3 aandachtspunten.
  In het rapport is tevens aangegeven dat in de broncode die bekeken is plaats is voor verbetering:[49] "*We adviseren om de huidige code volledig op te schonen of om deze te herschrijven zodat deze overzichtelijker en consistenter opgezet kan worden*."

In de brief van 13 februari 2013 aan het CBP stelt VCD "*De resultaten van de audit van Humannet Starter geven aan dat Humannet Starter goed beschermd is tegen ongeoorloofd gebruik van buitenaf. De zeer uitgebreide broncode check van Humannet Starter heeft gezorgd voor aanbevelingen die momenteel door medewerkers van VCD Humannet worden verwerkt. Zodra de aanbevelingen zijn doorgevoerd zal de Crystal Box audit voor Humannet Starter afgerond worden. Wij zullen u blijven informeren over de status en de resultaten*."

Het CBP heeft VCD gevraagd naar een audit waaruit blijkt dat de geconstateerde kwetsbaarheden in Humannet Starter zijn opgelost.[50]
Het CBP heeft tot de vaststelling van de voorlopige bevindingen geen audit van Humannet Starter ontvangen waaruit dit blijkt, ondanks herhaaldelijke verzoeken hiertoe.[51]

In de brief van 17 juni 2014 aan het CBP geeft VCD aan dat er inmiddels is gestart met penetratietesten door [Naam bedrijf]. Een tussentijdse rapportage (16 mei 2014) van

[45] [Naam bedrijf, naam rapport], versie 0.2, 21 december 2012, pag.1.
[46] [Naam bedrijf, naam rapport], *versie 1.0, 27 juli 2012*'.
[47] De beoordeling door deze externe partij gaat uit van een normenkader dat is gebaseerd op best practices. Zie: [Naam bedrijf, naam rapport], *versie 1.0, 27 juli 2012*' pag.1 en pag. 100.
[48] [Naam bedrijf, naam rapport], *27 juli 2012*', o.a. vanaf pag. 88.
[49] [Naam bedrijf, naam rapport], *27 juli 2012*', pag. 2, 3 en 87.
[50] In de e-mail van 4 april 2013 van VCD aan het CBP stelt VCD: "[…] *Naast deze rapportage zijn er geen andere*."
[51] Brief van 28 februari 2013 van het CBP aan VCD, brief van 28 maart 2013 van het CBP aan VCD en brief van 17 december 2013 van het CBP aan VCD .

een 'black box' penetratietest van Humannet starter is bijgevoegd in de bijlage[52] bij de brief. In deze penetratietest worden 5 gemiddelde risico's en 2 lage risico's geïdentificeerd, waaronder de mogelijkheid voor [risico][53], [risico][54] en [risico][55]. In de rapportage[56] wordt aangegeven dat er wordt gekeken of dit probleem kan worden opgelost door gebruik te maken van een oplossing van de hostingprovider.

Humannet Verzuim
Ten aanzien van de beveiliging van Humannet Verzuim wordt in de audits van Humannet Verzuim[57] [58] geconcludeerd:

- 22 juni 2012: de beveiliging van Humannet Verzuim is *'zeer onveilig*'. In de audit[59] staat: "*Doordat we een aantal kwetsbaarheden hebben gevonden waarvan uitbuiting grote gevolgen kan hebben, beoordelen we de applicatie als zeer onveilig.*"[60] Uit de audit[61] blijkt dat er 5 hoge risico's zijn aangetroffen:
    - [risico];
    - [risico];
    - [risico],
    - [risico] en
    - [risico].

  Voorts zijn er in de audit 6 gemiddelde risico's aangetroffen, 15 lage risico's en 6 aandachtspunten.
- 21 december 2012 (concept heronderzoek): de beveiliging van Humannet Verzuim is 'nipt voldoende'. In de audit[62] staat: " *Het hoge risico is opgelost, van de 8 gemiddelde risico's is 1 risico onopgelost. Van de 29 lage risico's blijven 19 risico's bestaan en van de 8 aandachtspunten blijven er 5 bestaan. Een laag risico is geïntroduceerd. We beoordelen de veiligheid van de applicatie als nipt voldoende.*"[63]

Bij brief van 17 juni 2014 heeft het CBP het definitieve heronderzoek[64] van 25 februari 2013 van bovengenoemd rapport ontvangen. De conclusies ten aanzien van de bovengenoemde kwetsbaarheden zijn niet gewijzigd ten opzichte van het concept heronderzoek van 21 december 2012.

In de brieven van 30 november 2013 en 15 januari 2014 stelt VCD dat zij diverse maatregelen heeft getroffen naar aanleiding van de audits die door [Naam bedrijf] zijn uitgevoerd. Dit betreft onder andere een Intrusion Prevention System (IPS), een Intrusion Detection System (IDS), [soort] Monitoring door [Naam bedrijf] en een softwarefilter.

---

[52] Bijlage 10 – 20140513-tussentijdse-rapportage-humannet-blackbox.
[53] Risico A3.1.
[54] Risico A8.1.
[55] Risico A10.1.
[56] Bijlage 11 – 20140616 [Naam bedrijf] – Human Starter status juni 2014.
[57] [Naam bedrijf, naam rapport], *versie 0.2, 22 juni 2012*'.
[58] [Naam bedrijf, naam rapport], *versie 0.2, 21 december 2012*'.
[59] [Naam bedrijf, naam rapport], *22 juni 2012*', pag. 2.
[60] De beoordeling door deze externe partij gaat uit van een normenkader dat is gebaseerd op best practices. Zie: [Naam bedrijf, naam rapport], *versie 0.2, 22 juni 2012*', pag.1 en pag. 81.
[61] [Naam bedrijf, naam rapport], *22 juni 2012*', vanaf pag. 72.
[62] [Naam bedrijf, naam rapport], *concept versie 0.2, 21 december 2012*'.
[63] De beoordeling door deze externe partij gaat uit van een normenkader dat is gebaseerd op best practices. Zie [Naam bedrijf, naam rapport], *concept versie 0.2, 21 december 2012*', pag.1 en pag. 59.
[64] [Naam bedrijf, naam rapport], *definitief versie 1.0, 25 februari 2013*'. Zoals blijkt uit het documentbeheer in het rapport (pag.iii) is dit een definitieve versie van het rapport dat op 20-12-2012 is opgesteld en op 21-12-2012 intern is gereviewd.

In de brief van 13 februari 2013 van VCD aan het CBP stelt VCD: "*Na een intensieve periode van samenwerking tussen medewerkers van VCD Humannet en [Naam bedrijf], is geconstateerd dat de mate van beveiliging van Humannet Verzuim en Humannet Starter meer dan voldoende is. De mate van veiligheid van online softwareoplossingen is aan te duiden in een vijftal categorieën, van 'Kritiek' tot en met 'Sterk'. Humannet Verzuim valt op dit moment in de categorie 'Voldoende' en zit daarmee in de vierde categorie. Dit geeft aan dat Humannet Verzuim goed beveiligd is tegen zowel extern als intern misbruik*."

In de brief van 30 november 2013 van VCD aan het CBP stelt VCD: "*In Humannet Verzuim heeft [Naam bedrijf] een aantal risico's geclassificeerd als hoog, hiervoor zijn passende maatregelen doorgevoerd in onze applicatie en infrastructuur. Ook de overige risico's geclassificeerd als 'gemiddeld' of 'laag', zijn volledig opgelost en in de re-audit gecontroleerd en geaccordeerd door [Naam bedrijf].*"

Het CBP heeft in de brief van 17 december 2013 aan VCD Humannet verzocht het bewijs toe te sturen waaruit blijkt dat [Naam bedrijf] of een andere externe partij bevestigt dat de geconstateerde kwetsbaarheden in Humannet Verzuim zijn opgelost, zoals VCD stelt in de brief van 30 november 2013.

Het CBP heeft hierop van VCD geen rapport van [Naam bedrijf] of een andere externe partij ontvangen.
In de brief van 17 juni 2014 aan het CBP stelt VCD: "*Helaas berust de zinsnede uit onze brief van 30 november 2013, dat "de overige risico's, geclassificeerd als 'gemiddeld' of 'laag', zijn volledig opgelost en in de re-audit gecontroleerd en geaccordeerd door [Naam bedrijf]" op een vervelend (intern) misverstand.*"

VCD stelt in de brief van 15 januari 2014 aan het CBP: "*Ondanks al deze maatregelen blijft het CBP aandringen op de oplossing van alle kwetsbaarheden. Echter, in de ogen van VCD Humannet dreigt er een spraakverwarring te ontstaan tussen enerzijds de 'passende maatregelen' conform artikel 13 Wbp en anderzijds het oplossen van alle kwetsbaarheden ongeacht het risico, zoals aangereikt door [Naam bedrijf]. Het CBP lijkt op dit punt van VCD Humannet te verlangen dat zij 'onkwetsbare' of 'feilloze' software dient te leveren. Bovendien is beveiliging een dynamisch proces omdat dagelijks nieuwe gevaren ontstaan. Foutloze software is, zoals algemeen bekend, een utopie*[65]*. Foutloze en onkwetsbare software is echter wel een continu streven van VCD Humannet, maar gaat de wettelijke eis van 'passende maatregelen' echter te buiten.*[…]".

In de brief van 15 januari 2014 geeft VCD aan dat [Naam bedrijf] binnenkort de software-oplossingen van VCD Humannet en VCD Starter opnieuw aan audits zullen onderwerpen. "*Het CBP zal vanzelfsprekend van deze audits op de hoogte worden gebracht. [...] Vanwege de implementatie van sterke authenticatie in het vierde kwartaal van 2013 heeft VCD Humannet besloten om de audit uit te stellen*."

In de brief van 17 juni 2014 aan het CBP geeft VCD aan dat zij [Naam bedrijf] heeft ingeschakeld om penetratietesten uit te voeren. De penetratietesten zijn op het moment van het schrijven van de brief van 17 juni 2014 in gang.

[65] Vgl. https:/ / nl.wikipedia.org/ wiki/ Testen_(software) (januari 2014).

Ten aanzien van de geconstateerde kwetsbaarheden in het heronderzoek van 21 december 2012 geeft VCD in bijlage 2 bij de brief van 17 juni 2014 aan welke opvolging zij heeft gegeven aan de kwetsbaarheden.[66] Bij een aantal kwetsbaarheden[67] die zijn geconstateerd in het heronderzoek van 21 december 2012 staat de opmerking: "*Vanuit de penetratietesten van [Naam bedrijf] zal moeten blijken of dit risico nog bestaat*." Bij een groot aantal kwetsbaarheden[68] die zijn geconstateerd in het heronderzoek van 21 december 2012 staat '*oplossing niet onderzocht*'.
In de brief van 17 juni 2014 geeft VCD aan dat zij voor Humannet Starter en Humannet Verzuim de volgende maatregelen heeft getroffen:

- implementatie van een Information Security Management System (ISMS);
- certificering van het ISMS aan de hand van de norm NEN-ISO/ IEC 27001,[69]
- de inrichting van een intern security team "*dat zorgdraagt voor continue implementatie en aanpassingen van beveiligingsmaatregelen die door een iteratieve procedure doorlopend worden aangescherpt*. […] *Op advies van het security team hebben wij inmiddels één full-time programmeur/software-ontwikkelaar beschikbaar voor de implementatie van de maatregelen*."

[66] 20140616 – bijlage 2 – MG – Humannet Verzuim status juni 2014.
[67] Gemiddeld risico 8, laag risico 3 en 6.
[68] Laag risico 2, 3,6, 7, 8, 11, 16, 17, 18, 19, 21, 22, 23, 25, 27 en aandachtspunt 2 en 3.
[69] Vgl. http:/ / 17799.standardsdirect.org/ (juli 2014), NEN-ISO/ IEC 27001 is een specificatie voor een ISMS die de basis vormt voor een audit en certificering door een derde partij.

4 BEOORDELING VOORLOPIGE BEVINDINGEN

Onderstaand volgt de integrale tekst zoals deze is opgenomen in de beoordeling van het rapport voorlopige bevindingen.

Verwerking van persoonsgegevens

Volgens artikel 1, aanhef en onder a, van de Wbp wordt onder een 'persoonsgegeven' verstaan *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*.

'Verwerking van persoonsgegevens' is gedefinieerd in artikel 1, aanhef en onder b, van de Wbp als "*elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.*"

Binnen de applicatie Humannet Starter en Humannet Verzuim worden gegevens verwerkt van werknemers.[70] Het betreft onder andere naam, adres, woonplaats en medische en verzuimdossiers.
Deze gegevens hebben betrekking op geïdentificeerde natuurlijke personen, de werknemers die geregistreerd staan in Humannet Starter en Humannet Verzuim. Bovengenoemde gegevens zijn derhalve persoonsgegevens als bedoeld in artikel 1, onder a, Wbp.

Verantwoordelijke en bewerker

Op grond van artikel 1, aanhef en onder d, van de Wbp is de verantwoordelijke *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*.

Op grond van artikel 1, aanhef en onder e, van de Wbp is de bewerker *degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderwerpen*.

De werkgevers en arbodiensten registreren de (medische) persoonsgegevens in Humannet Starter en Humannet Verzuim in het kader van de begeleiding en re-integratie van zieke werknemers.

Op de website van VCD staat over Humannet Verzuim en Humannet Starter:[71]
"*Met onze verzuimsoftware geeft u uw verzuimbeleid perfect vorm. Samen met u stellen wij het ideale verzuimsysteem samen. Een verzuimsysteem dat perfect aansluit bij de processen binnen uw organisatie en rekening houdt met uw eisen en wensen.*"

In de antwoorden op vragen van het CBP aan de onderzochte organisaties die gebruik maken van Humannet Starter is het volgende aangegeven:

- de applicatie draait bij VCD;[72] [73] [74]

[70] Brief van 27 april 2012 van VCD aan het CBP en e-mail van 28 april 2014 van VCD aan het CBP.
[71] http://www.vcdhumannet.nl/verzuimsoftware, 12 mei 2014.
[72] Brief van 31 oktober 2013 van klant 2 aan het CBP, antwoord op vraag 5.
[73] Brief van 13 januari 2013 van klant 3 aan het CBP, antwoord op vraag 5.

- het operationeel en technisch beheer ligt bij VCD ligt;[75] [76] [77] en
- VCD heeft toegang tot de gegevens in Humannet Starter en Humannet Verzuim.[78] [79] [80]

Uit bovenstaande blijkt dat VCD het systeem ter beschikking stelt en het beheer (waaronder de beveiliging) van de applicaties uitvoert.
Dit betekent tevens dat VCD de (medische) gegevens verwerkt. Zo schermt VCD onder andere de gegevens af voor onbevoegden en stelt VCD de gegevens ter beschikking aan de klanten (door toegang te verlenen). Tevens staan de gegevens bij VCD op de server. VCD bewaart derhalve de (medische) persoonsgegevens voor de verantwoordelijken en heeft toegang tot de gegevens. Zij kan de gegevens derhalve onder andere bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verspreiden, samenbrengen, uitwissen of vernietigen. Ook dit zijn verwerkingen van persoonsgegevens zoals bedoeld in artikel 1, aanhef en onder b, van de Wbp.

De klanten die de applicaties gebruiken bepalen het doel (de begeleiding en re-integratie van zieke werknemers) en de middelen (onder andere de inzet van Humannet Verzuim of Humannet Starter) om dit doel te bereiken.

Hieruit volgt dat de klanten van Humannet Starter en Humannet Verzuim worden aangemerkt als de verantwoordelijken voor de gegevensverwerking in de applicaties, en dat VCD de bewerker is, die de applicaties beheert voor haar klanten. De beveiliging vormt een onderdeel van het beheer.

Dit wordt door VCD zelf bevestigd in de brief van 6 juni 2013 van VCD aan de relaties en in de brief van 30 november 2013 van VCD aan het CBP waarin VCD stelt: "*De Wbp stelt eisen aan de vorm en de inhoud van de afspraken die een verantwoordelijke met een bewerker, in dit geval VCD Humannet, maakt en eist dat deze schriftelijk vastgelegd worden. Op 6 juni 2013 hebben wij aan onze relaties een brief gezonden (zie bijlage 4) waarin de werking van de Wbp en de termen 'verantwoordelijke' en 'bewerker' zijn toegelicht. Bijgevoegd hebben wij een bewerkersovereenkomst waarin alle door de Wbp opgelegde verplichtingen met betrekking tot het verwerken van persoonsgegevens zijn opgenomen (zie bijlage 5). Door het ondertekenen van deze overeenkomst heeft onze klant als verantwoordelijke en als relatie van VCD Humannet alles goed geregeld.*" .

In dit kader moet worden benadrukt dat de rol van de bewerker bij de huidige complexe geautomatiseerde verwerkingen van persoonsgegevens niet passief kan zijn. Immers, omdat veel verantwoordelijken de specialistische kennis en kunde die nodig is voor een deugdelijke geautomatiseerde gegevensverwerking niet zelf in huis (kunnen) hebben, wordt een beroep gedaan op bewerkers die deze expertise wel hebben. Die rol brengt voor de bewerker een zekere verantwoordelijkheid met zich mee die hij actief moet invullen, bijvoorbeeld ten aanzien van het voldoende

[74] Brief van 10 november 2013 van de advocaat van klant 1 aan het CBP, antwoord op vraag 5.
[75] Brief van 31 oktober 2013 van klant 2 aan het CBP, antwoord op vraag 6.
[76] Brief van 13 januari 2013 van klant 3 aan het CBP, antwoord op vraag 6.
[77] Brief van 10 november 2013 van de advocaat van klant 1 aan het CBP, antwoord op vraag 6.
[78] Brief van 31 oktober 2013 van klant 2 aan het CBP, antwoord op vraag 9.
[79] Brief van 13 januari 2013 van klant 3 aan het CBP, antwoord op vraag 9.
[80] Brief van 10 november 2013 van de advocaat van klant 1 aan het CBP, antwoord op vraag 9.

beveiligen van de gegevensverwerking die hij beheert c.q. uitvoert ten behoeve van de verantwoordelijke.

Dit volgt ook uit de memorie van toelichting op artikel 1 Wbp, waar over de bewerker het volgende staat: "*Hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking door de bewerker (zie artikel 12), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens (hoofdstuk 1 en 2 van dit wetsvoorstel).*[81]

Beveiliging

Uit het juridisch kader (zie hoofdstuk 2) blijkt dat bij de verwerking van medische gegevens in de applicaties Humannet Starter en Humannet Verzuim in ieder geval de volgende eisen worden gesteld om aan de in artikel 13 Wbp gestelde 'passende maatregelen' uitvoering te geven:

Authenticatie:

1. toegang tot medische gegevens dient plaats te vinden middels meervoudige authenticatie.

Technische kwetsbaarheden:

2. beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht, bijvoorbeeld middels penetratietesten en/ of security scans;
3. er moeten (doorlopend) organisatorische en/ of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken;

Authenticatie

Ad1. Toegang tot medische gegevens dient plaats te vinden middels meervoudige authenticatie.

Zoals beschreven in het juridisch kader dient toegang tot een systeem waarin medische gegevens worden verwerkt altijd plaats te vinden middels meervoudige authenticatie.

In de brief van 16 mei 2012 aan het CBP stelt VCD dat zij, uiterlijk augustus 2012, een [soort] token als authenticatie toe gaat passen voor Humannet Starter en Humannet Verzuim voor alle relaties van VCD.

Tijdens het onderzoek van het CBP is de planning van de toepassing van meerfactor authenticatie meerdere keren door VCD[82] verzet naar een later tijdstip.[83] [84] [85] [86]

In de brief van 17 juni 2014 stelt VCD: "*Ten aanzien van onze klanten hebben wij ze allemaal aangeschreven met de mogelijkheid tot het afnemen van sterke authenticatie. Dit*

[81] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 61.
[82] Dit is zo door het CBP geconcludeerd in de voorlopige bevindingen van 7 augustus 2014. VCD heeft in de zienswijze van 11 september 2014 aangegeven dat het uitstel lag aan de implementatie van de [Naam software] bij de specifieke infrastructuur van de betreffende klant en dat het onjuist is dat dit aan VCD lag. Dit blijkt volgens VCD uit de e-mail van 26 juni 2014 van klant 3 aan VCD.
[83] Telefoongesprek van het CBP met VCD op 11 september 2012
[84] Telefoongesprek van het CBP met VCD op 6 februari 2013.
[85] Brief van 13 februari 2013 van VCD aan het CBP.
[86] Gevorderd door het CBP bij brief van 28 maart 2013.

leidde tot [aantal] offerteaanvragen, die zijn uitgemond in [aantal] getekende offertes, waarbij voor [aantal] de implementatie in volle gang is."

In dat verband is tevens van belang dat klant 3, die wel heeft aangegeven meerfactor authenticatie te willen toepassen, op 1 april 2014 heeft gemeld dat implementatie door VCD[87] is uitgesteld tot 1 juni 2014 en op 2 juli 2014 heeft gemeld dat de implementatiedatum weer is uitgesteld.

Uit bovenstaande leidt het CBP af dat meerfactor authenticatie door VCD slechts als mogelijkheid wordt aangeboden aan klanten, en derhalve geen vast onderdeel uitmaakt van de applicaties van Humannet Starter en Humannet Verzuim. De authenticatie is op dit moment nog niet ingevoerd bij gebruikers van Humannet Starter en Humannet Verzuim; bij [aantal] loopt op dit moment een implementatietraject.

Zoals in het juridisch kader is beschreven dient bij authenticatie bij de toegang tot medische gegevens tenminste gebruik te worden gemaakt van tweefactor authenticatie.[88]
Doordat niet alle klanten[89] gebruik maken van meerfactor authenticatie bij de toegang tot de medische gegevens in Humannet Starter en Humannet Verzuim wordt gehandeld in strijd met de vereisten ten aanzien van de beveiliging zoals die volgen uit artikel 13 Wbp.

Conclusie authenticatie
Uit het onderzoek blijkt dat VCD, die bewerker is, gegevens verwerkt in de applicaties Humannet Starter en Humannet Verzuim. VCD verzorgt onder andere de beveiliging van de applicaties Humannet Starter en Humannet Verzuim. De beveiliging van de applicaties voldoet niet aan de vereisten zoals deze ten aanzien van de beveiliging volgen uit artikel 13 Wbp omdat meerfactor authenticatie op dit moment nog niet is ingevoerd bij de gebruikers van Humannet Starter en Humannet Verzuim.[90]

In de memorie van toelichting op artikel 1 Wbp staat over de bewerker: "*Hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking door de bewerker (zie artikel 12), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens (hoofdstuk 1 en 2 van dit wetsvoorstel).*[91]
Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, is VCD op grond van bovenstaande aanspreekbaar op de tekortkomingen in de beveiliging van de applicatie.

---

[87] Dit is zo door het CBP geconcludeerd in de voorlopige bevindingen van 7 augustus 2014. VCD heeft in de brief van 11 september 2014 aangegeven dat het uitstel lag aan de implementatie van de [Naam software] bij de specifieke infrastructuur van de betreffende klant en dat het onjuist is dat dit aan VCD lag. Dit blijkt volgens VCD uit de e-mail van 26 juni 2014 van klant 3 aan VCD.
[88] Zie ook z2012-00623 'Onderzoek naar het gebruik van waarneemdossiers bij Stichting Gezondheidscentra Haarlemmermeer', CBP, augustus 2013.
[89] Op 2 juli 2014 maakt nog geen enkele klant gebruik van sterke authenticatie.
[90] In de brief van 2 juli van klant 3 is aangegeven dat op dat moment een implementatietraject loopt.
[91] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 61.

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt.
In de wetsgeschiedenis van artikel 6 Wbp is aangegeven het woord 'wet' mede betrekking heeft op andere wetgeving inzake de verwerking van persoonsgegevens. Het gaat hier dus om een schakelbepaling die verzekert dat de betrokken regelingen in onderling verband van toepassing zijn.[92]

VCD heeft op dit moment nog geen meerfactor authenticatie ingevoerd bij de gebruikers van Humannet Starter en Humannet Verzuim.[93] Hiermee voldoen de applicaties Humannet Starter en Humannet Verzuim niet aan de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens[94]. Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens zoals bedoeld in artikel 6 Wbp. Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

Technische kwetsbaarheden

Ad 2 Beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht middels penetratietesten en/ of security scans.
Ad 3. Er moeten (doorlopend) organisatorische en/ of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken.

Medische gegevens behoren tot de categorie bijzondere gegevens als bedoeld in artikel 16 Wbp. Medische gegevens van werknemers zijn zeer gevoelige gegevens. Dit betekent dat hoge eisen gesteld worden aan de technische en organisatorische maatregelen ter bescherming van deze gegevens.
Zoals VCD zelf ook stelt in de brief van 15 januari 2014 aan dat het CBP "*is beveiliging een dynamisch proces omdat dagelijks nieuwe gevaren ontstaan.*"

Zoals ook is vermeld in het juridisch kader (hoofdstuk 2) staat in de ICT-Beveiligingsrichtlijnen voor webapplicaties van het NCSC[95] onder andere de beveiligingsrichtlijn dat penetratietesten en audits periodiek moeten worden uitgevoerd.
Hierbij wordt niet aangegeven wat wordt verstaan onder 'periodiek'. Beveiliging is, zoals VCD zelf ook aangeeft, een dynamisch proces is waarin dagelijks nieuwe risico's ontstaan. Deze kunnen bijvoorbeeld ontstaan door kwetsbaarheden in nieuwe software, door kwetsbaarheden in verouderde software maar ook doordat er door de beheerder zelf doorlopend aanpassingen aan het systeem/ de applicaties worden gedaan. Doordat er doorlopend nieuwe risico's kunnen ontstaan is het CBP van oordeel dat het passend is, om zeker in het geval van een applicatie waarin medische gegevens worden verwerkt, meerdere penetratietesten/ scans per jaar uit te voeren.[96]

[92] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 78.
[93] In de brief van 2 juli van klant 3 is aangegeven dat op dat moment een implementatietraject loopt.
[94] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.
[95] Deel 1, januari 2012, pag. 17.
[96] Dit kunnen zowel testen zijn die door externe partijen worden uitgevoerd, of testen die intern worden uitgevoerd.

In de brief van 27 april 2012 van VCD aan het CBP heeft Humannet aangegeven dat er elk jaar zowel voor Humannet Starter als voor Humannet Verzuim een uitgebreide audit zal worden uitgevoerd.

Het uitvoeren van een jaarlijkse audit, zoals de door Humannet gebruikte Black Box/ Grey Box, kan onder omstandigheden passend zijn om de beveiligingsrisico's in kaart te brengen aangezien dit een zeer uitgebreide audit betreft.

De uitvoering van een uitgebreide audit kan als passend worden gekwalificeerd indien:

- de uitgebreide audit periodiek plaatsvindt, minimaal 1 keer per jaar;
- er tevens andere beveiligingsmaatregelen in worden gezet om beveiligingsrisico's doorlopend in kaart te brengen, zoals IDS en het [soort] Monitoring door [Naam bedrijf], waar VCD gebruik van maakt; en
- voldoende opvolging wordt gegeven aan de in de jaarlijks uitgevoerde en bovengenoemde uitgebreide audit geconstateerde kwetsbaarheden.

Onderstaand wordt getoetst of de maatregelen die VCD heeft genomen ten aanzien van beide applicaties passend zijn. Hierbij wordt eerst ingegaan op de frequentie van de audits, vervolgens wordt ingegaan op de maatregelen die zijn getroffen om de geconstateerde risico's zoveel mogelijk te beperken.

Humannet Starter
Ad 2 Beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht middels penetratietesten en/ of security scans.

Ten aanzien van Humannet Starter heeft één audit plaatsgevonden op 27 juli 2012. Bij e-mail van 4 april 2013 heeft VCD aangegeven geen (her)audit van Humannet Starter te hebben uitgevoerd.
In de brief van 15 januari 2014 van VCD is aangegeven dat een voorgenomen audit is uitgesteld.
In de brief van 17 juni 2014 stelt VCD dat er op dat moment penetratietesten plaatsvinden en is een tussentijdse rapportage bijgevoegd.

Uit bovenstaande blijkt dat voor Humannet Starter de laatste (en enige) audit in 2012 heeft plaatsgevonden. Hiermee is geen gevolg gegeven aan de voorwaarde die volgt uit artikel 13 Wbp en de richtsnoeren beveiliging van het CBP dat beveiligingsrisico's (doorlopend) in kaart dienen te worden gebracht middels penetratietesten en/ of security scans. Immers, het uitvoeren van een jaarlijkse uitgebreide audit, zoals de door Humannet gebruikte Black Box/ Grey Box kan slechts als passend worden gekwalificeerd indien tenminste aan de voorwaarde is voldaan dat de uitgebreide audit minimaal 1 keer per jaar plaatsvindt.[97] Aangezien in 2013 geen audit voor Humannet Starter heeft plaatsgevonden en de audit uit 2014 nog niet is afgerond wordt niet aan deze voorwaarde voldaan.

Ad 3. Er moeten (doorlopend) organisatorische en/ of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken.

[97] Zie paragraaf 'technische kwetsbaarheden', pag. 24.

In de audit van 27 juli 2012 is de beveiliging van Humannet Starter als '*zeer onveilig*' aangemerkt. Uit de audit[98] blijkt dat er 5 hoge risico's, 6 gemiddelde risico's, 25 lage risico's en 3 aandachtspunten zijn aangetroffen.

In de brief van 13 februari 2013 stelt VCD ten aanzien van Humannet Starter: "*De resultaten van de audit van Humannet Starter geven aan dat Humannet Starter goed beschermd is tegen ongeoorloofd gebruik van buitenaf.*
Het CBP heeft geen audit ontvangen waaruit blijkt dat Humannet Starter op dat moment passend beschermd is tegen ongeoorloofd gebruik van buitenaf.

Bij brief van 27 juni 2014 heeft het CBP een tussentijdse rapportage ontvangen van een penetratietest van 16 mei 2014 van Humannet starter. In deze penetratietest worden 5 gemiddelde risico's en 2 lage risico's geïdentificeerd, waaronder de mogelijkheid [risico][99], [risico][100] en [risico][101].
In de brief van 27 juni 2014 van VCD aan het CBP[102] geeft VCD aan dat er samen met de hostingprovider wordt onderzocht of deze kwetsbaarheden kunnen worden opgelost door gebruik te maken van een oplossing van de hostingprovider. In de brief is niet aangegeven op welke termijn de kwetsbaarheden zullen worden opgelost en of er andere alternatieven zijn om de geconstateerde kwetsbaarheden op te lossen of te beperken.

VCD heeft gedurende het onderzoek van het CBP diverse technische en organisatorische maatregelen getroffen om de beveiliging van de applicaties Humannet Starter en Humannet Verzuim te verbeteren. Dit betreft onder andere een Intrusion Prevention System (IPS), een Intrusion Detection System (IDS), [soort] Monitoring door [Naam bedrijf], een softwarefilter, implementatie van ISMS en de norm NEN-ISO/ IEC 27001 en de inrichting van een intern security team.

Ondanks deze door VCD getroffen maatregelen blijkt uit de penetratietest van 16 mei 2014 dat ook nu weer gebruik kan worden gemaakt van [risico], wat, in combinatie met [risico] en [risico], een risico vormt op ongeautoriseerde toegang tot Humannet Starter. Risico's dienen te worden geïnterpreteerd in de context van het systeem. Omdat in Humannet Starter medische gegevens worden verwerkt, is dit risico onacceptabel.
Aan de geconstateerde kwetsbaarheid is in ieder geval tot het moment van de brief van VCD aan het CBP van 17 juni 2014 onvoldoende adequate opvolging gegeven. De kwetsbaarheid is nog niet opgelost. Het is voorts niet duidelijk of de kwetsbaarheid op de voorgestelde manier kan worden opgelost[103] en of er alternatieven zijn. Ook is geen tijdspad aangegeven waarin de kwetsbaarheid zal worden opgelost.

De beveiliging van Humannet Starter voldoet derhalve niet aan de eis dat er (doorlopend) organisatorische en/ of technische maatregelen moeten worden getroffen

[98] [Naam bedrijf, naam rapport], *27 juli 2012*', o.a. vanaf pag. 88.
[99] Risico A3.1.
[100] Risico A8.1.
[101] Risico A10.1.
[102] Brief van 17 juni van VCD aan het CBP 2014, bijlage 2.
[103] Het feit dat VCD voor de voorgestelde oplossing afhankelijk is van een externe partij, maakt het risico groter omdat VCD minder invloed heeft.

om de geconstateerde risico's zoveel mogelijk te beperken en daarmee een passend beveiligingsniveau te garanderen.

Conclusie technische kwetsbaarheden Humannet Starter
Uit het onderzoek blijkt dat VCD, die bewerker is, gegevens verwerkt in de applicatie Humannet Starter. VCD verzorgt onder andere de beveiliging van de applicatie Humannet Starter. Artikel 13 Wbp bepaalt dat passende maatregelen moeten worden getroffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Hieruit volgt dat beveiligingsrisico's (doorlopend) in kaart dienen te worden gebracht middels penetratietesten en/ of security scans. Daarnaast moeten er (doorlopend) organisatorische en/ of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken.
De beveiliging van de applicatie Humannet Starter voldoet niet aan de vereisten zoals deze ten aanzien van de beveiliging volgen uit artikel 13 Wbp omdat voor Humannet Starter geen periodieke audits hebben plaatsgevonden en onvoldoende adequate opvolging is gegeven aan de kwetsbaarheden die zijn geconstateerd in de audit van 16 mei 2014.

In de memorie van toelichting op artikel 1 Wbp staat over de bewerker: "*Hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking door de bewerker (zie artikel 12), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens (hoofdstuk 1 en 2 van dit wetsvoorstel).*[104]
Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, is VCD op grond van bovenstaande aanspreekbaar op de tekortkomingen in de beveiliging van de applicatie.

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt.
In de wetsgeschiedenis van artikel 6 Wbp is aangegeven het woord 'wet' mede betrekking heeft op andere wetgeving inzake de verwerking van persoonsgegevens. Het gaat hier dus om een schakelbepaling die verzekert dat de betrokken regelingen in onderling verband van toepassing zijn.[105]

Voor Humannet Starter hebben geen periodieke audits plaatsgevonden en is onvoldoende opvolging gegeven aan de kwetsbaarheden die zijn geconstateerd in de audit van 16 mei 2014. Hiermee voldoet de applicatie Humannet Starter niet aan de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens.[106] Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens zoals bedoeld in artikel 6 Wbp. Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

[104] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 61.
[105] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 78.
[106] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.

Humannet Verzuim
Ad 2 Beveiligingsrisico's dienen (doorlopend) in kaart te worden gebracht middels penetratietesten en/ of security scans.

Ten aanzien van Humannet Verzuim heeft er een uitgebreide audit plaatsgevonden op 22 juni 2012 en een heronderzoek op 21 december 2012 (die definitief is gemaakt op 25 februari 2013). Tijdens het onderzoek van het CBP heeft VCD geen documenten aangeleverd waaruit blijkt dat er audits hebben plaatsgevonden in 2013. In de brief van 15 januari 2014 geeft VCD aan dat een voorgenomen audit is uitgesteld.
In de brief van 17 juni 2014 stelt VCD dat er op dat moment penetratietesten plaatsvinden.

Uit bovenstaande blijkt dat voor Humannet Verzuim één audit en één heronderzoek heeft plaatsgevonden, beide in 2012. Hiermee is geen gevolg gegeven aan de voorwaarde die volgt uit artikel 13 Wbp en de richtsnoeren beveiliging van het CBP dat beveiligingsrisico's (doorlopend) in kaart dienen te worden gebracht middels penetratietesten en/ of security scans. Immers, het uitvoeren van een jaarlijkse uitgebreide audit, zoals de door Humannet gebruikte Black Box/ Grey Box kan slechts als passend worden gekwalificeerd indien tenminste aan de voorwaarde is voldaan dat de uitgebreide audit minimaal 1 keer per jaar plaatsvindt.[107] Aangezien in 2013 geen audit voor Humannet Verzuim heeft plaatsgevonden en de audit uit 2014 nog niet is afgerond wordt niet aan deze voorwaarde voldaan.

Ad 3. Er moeten (doorlopend) organisatorische en/ of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken.

De laatst feitelijk vernomen situatie over de stand van de beveiliging van Humannet Verzuim is afkomstig van een externe partij en betreft de situatie in het heronderzoek van 21 december 2012 en 25 februari 2013, waarin de beveiliging van Humannet Verzuim als '*nipt voldoende*' wordt aangemerkt en waarin nog 1 gemiddeld risico, 19 lage risico's en 5 aandachtspunten niet zijn opgelost.

Het CBP heeft VCD Humannet tijdens het onderzoek verzocht aan te geven hoe zij opvolging heeft gegeven aan de geconstateerde kwetsbaarheden en tevens aan te tonen dat de kwetsbaarheden zijn opgelost of, indien de kwetsbaarheden niet zijn opgelost, aan te geven welke afweging hieraan vooraf is gegaan. VCD heeft niet aangetoond dat de kwetsbaarheden zijn opgelost. Bij een aantal kwetsbaarheden[108] die zijn geconstateerd in het heronderzoek van 21 december 2012 staat in de brief van VCD van 17 juni 2014 de opmerking: "*Vanuit de penetratietesten van [Naam bedrijf] zal moeten blijken of dit risico nog bestaat.*" Bij een groot aantal kwetsbaarheden[109] die zijn geconstateerd in het heronderzoek van 21 december 2012 staat "*oplossing niet onderzocht*".

Beveiliging is een dynamisch proces is waarin dagelijks nieuwe risico's ontstaan, bijvoorbeeld door kwetsbaarheden in nieuwe software, door kwetsbaarheden in verouderde software maar ook doordat de beheerder zelf doorlopend aanpassingen

[107] Zie paragraaf 'technische kwetsbaarheden', pag. 24.
[108] Gemiddeld risico 8, laag risico 3 en 6.
[109] Laag risico 2, 3,6, 7, 8, 11, 16, 17, 18, 19, 21, 22, 23, 25, 27 en aandachtspunt 2 en 3.

aan het systeem/ de applicaties heeft gedaan. Doordat er vanaf 21 december 2012 doorlopend nieuwe risico's kunnen zijn ontstaan in Humannet Verzuim en er geen nieuwe audit heeft plaatsgevonden in 2013, en de audit in 2014 nog niet is afgerond, bestaat geen inzicht in de actuele stand van de risico's en de maatregelen die in dat kader getroffen zouden moeten worden.

Conclusie technische kwetsbaarheden Humannet Verzuim
Uit het onderzoek blijkt dat VCD, die bewerker is, gegevens verwerkt in de applicatie Humannet Verzuim. VCD verzorgt onder andere de beveiliging van de applicatie Humannet Verzuim. Artikel 13 Wbp bepaalt dat passende maatregelen moeten worden getroffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Hieruit volgt dat beveiligingsrisico's (doorlopend) in kaart dienen te worden gebracht middels penetratietesten en/ of security scans. Daarnaast moeten er (doorlopend) organisatorische en/ of technische maatregelen worden getroffen om de geconstateerde risico's zoveel mogelijk te beperken.

De beveiliging van de applicatie Humannet Verzuim voldoet niet aan de vereisten zoals deze ten aanzien van de beveiliging volgen uit artikel 13 Wbp omdat voor Humannet Verzuim geen periodieke audits hebben plaatsgevonden. Hierdoor bestaat momenteel geen inzicht in de huidige stand van de risico's en de maatregelen die in dat kader getroffen zouden moeten worden.

In de memorie van toelichting op artikel 1 Wbp staat over de bewerker: "*Hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking door de bewerker (zie artikel 12), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens (hoofdstuk 1 en 2 van dit wetsvoorstel).*[110]
Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, is VCD op grond van bovenstaande aanspreekbaar op de tekortkomingen in de beveiliging van de applicatie.

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt.
In de wetsgeschiedenis van artikel 6 Wbp is aangegeven het woord 'wet' mede betrekking heeft op andere wetgeving inzake de verwerking van persoonsgegevens. Het gaat hier dus om een schakelbepaling die verzekert dat de betrokken regelingen in onderling verband van toepassing zijn.[111]

Voor Humannet Verzuim hebben geen periodieke audits plaatsgevonden. Hierdoor bestaat geen inzicht in de actuele stand van de risico's en de maatregelen die in dat kader getroffen zouden moeten worden. Hiermee voldoet de applicatie Humannet Verzuim niet aan de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens.[112] Er is derhalve

[110] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 61.
[111] Kamerstukken II 1997/ 98, 25 892, nr. 3, p. 78.
[112] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.

sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens, zoals bedoeld in artikel 6 Wbp.
Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

5 ZIENSWIJZE VCD

Bij brief van 11 september 2014 heeft VCD, bij monde van haar advocaat, haar zienswijze gegeven op het rapport voorlopige bevindingen.

In de zienswijze stelt VCD dat de invulling aan artikel 13 Wbp door het CBP disproportioneel is om de volgende redenen:

1. "*Proportionaliteit dient ook betrekking te hebben op de kosten*".

   VCD stelt in de zienswijze dat VCD niet betwist "*dat medische gegevens een hogere gevoeligheid hebben en dat derhalve aan beveiliging daarvan hogere eisen kunnen worden gesteld dan aan bijvoorbeeld NAW-gegevens. Wel gaat het CBP in haar concept-rapport voorbij aan het feit dat de te nemen maatregelen ook proportioneel dienen te zijn in relatie tot de te maken 'kosten van de tenuitvoerlegging'*." Dat blijkt volgens VCD niet alleen uit de tekst van artikel 13 Wbp, maar ook uit de tekst op de website van het CBP: *"[…]kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist*."
   VCD stelt voorts: "*Ook de wetgever heeft over vereisten aan informatiebeveiliging reeds tijden terug geconstateerd en overwogen dat absolute beveiliging een utopie is en dat maximale beveiliging niet verlangd kan worden omdat 'het onzinnig is een gulden te beveiligen met een rijksdaalder.'(Kamerstukken II 1989/90, 21 551, nr. 3, p.16.)*"

VCD stelt dat zij dit punt meerdere keren heeft aangedragen maar het punt noch de onderbouwde weerlegging niet terug kan vinden in het rapport voorlopige bevindingen. VCD verwijst hierbij naar de brief van 15 januari 2014.

Voorts maakt het CBP volgens VCD "*onvoldoende onderscheid tussen een grotere groep gebruikers (ca. [aantal] personen) die toegang heeft tot niet-medische gegevens, en een veel kleinere groep van (arbo)artsen (zo'n [aantal] personen) die wel toegang krijgen tot medische gegevens, terwijl dit aspect ook bij de proportionaliteit van de kosten dient te worden meegewogen*."[113]

Tot slot stelt VCD dat dit kostenaspect ook een rol heeft gespeeld bij de vertraging van de invoering van meerfactor authenticatie. "*Het betrof een sterk authenticatieplatform van leverancier [Naam bedrijf], waarvan later bleek dat de hoge investering in geen verhouding staat tot de opbrengsten en de bedrijfscontinuïteit ernstig in gevaar zou brengen. Hierdoor is vertraging opgelopen voordat cliënte het platform van [Naam software] heeft geïmplementeerd als meer betaalbaar en veilig alternatief."*

2. "*NEN 7510-norm als onjuiste toetsingsgrondslag gebruikt door CBP*".

   VCD stelt dat de NEN 7510-norm geen betrekking heeft op bewerkers van verzuimgegevens en door het CBP als onjuiste toetsingsgrond is gebruikt.

[113] E-mail van 21 oktober van de advocaat van VCD aan het CBP.

VCD stelt dat dit blijkt uit de uitspraak van de Centrale Raad van Beroep[114] waarin staat:
"*De NEN 7510 norm is een gezaghebbende sectorale uitwerking van art. 13 Wbp; als een ziekenhuis voldoet aan de NEN 7510 norm, mag ervan uit worden gegaan dat het ook voldoet aan bovengenoemde wettelijke bepaling. Andersom is dit overigens geen volstrekt automatisme: een ziekenhuis kan ook op andere wijze aantonen dat de beveiliging in orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging (ISO 17799).*"
VCD stelt dat uit deze informatie blijkt dat de NEN 7510 norm een sectorale uitwerking is, dus voor zorginstellingen, en derhalve niet zondermeer verbindend is voor cliënte.
VCD stelt dat dit ook blijkt uit de informatie van NEN zelf op haar website waarop staat:
"*NEN 7510 beschrijft een set maatregelen dat zorginstellingen moeten treffen om via een gecontroleerd proces op adequate wijze met (medische) gegevens moeten omgaan*".

Tevens stelt VCD dat deze norm enkel te koop is bij NEN en niet publiekelijk vrijelijk beschikbaar en openbaar is en dat het ook op deze grond onjuist is dat het CBP toch deze norm voorschrijft aan cliënte. "*Algemeen afdwingbare wetten, regels en normen dienen inhoudelijk volledig publiekelijk toegankelijk te zijn*."

3. "*De meervoudige authenticatie is door het CBP ontleend aan beveiligings-standaarden die niet gelden voor cliënte*".

VCD geeft aan dat zij van mening is dat medische gegevens goed beveiligd dienen te worden en dat meervoudige authenticatie zeer goede beveiliging biedt. VCD stelt vervolgens dat de door het college aangehaalde eis dat informatiesystemen die patiëntgegevens verwerken, authenticatie behoren toe te passen op basis van tenminste twee afzonderlijke kenmerken, voor zorginstellingen geldt, en niet voor VCD. "*De vereenzelviging tussen een zorginstelling en een bewerker van verzuimgegevens is zonder nadere onderbouwing niet te volgen*."

VCD stelt dat de norm voor betrouwbaarheidsniveau 3 (STORK QAA niveau 3), die is ontleend aan de "Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten" van Forum Standaardisatie, geldt voor elektronische overheidsdiensten en niet voor VCD.

Tevens laat het CBP volgens VCD na te motiveren waarom het STORK-raamwerk als leidend en geldend dient te worden beschouwd, terwijl VCD de Afhankelijkheids- en Kwetsbaarheidsanalyse heeft toegepast in het kader van het ISO 27001-certificeringstraject.

VCD stelt: "*Medische gegevens worden in het kader van niet-zorginstellingen en niet-overheidsdiensten afdoende geborgd door een gedegen informatiebeveiligingsbeleid dat voldoet aan NEN-ISO/IEC 27001*."

[114] CRvB 1 juli 2008, WBP 2009, afl. 1.

Voorts geeft VCD aan dat zij desalniettemin Humannet Starter en Humannet Verzuim wel reeds heeft ingericht voor het gebruik van meervoudige authenticatie en dit "*uitdrukkelijk aangeboden en geadviseerd*" aan haar klanten. VCD stelt in de zienswijze dat zij al haar klanten gaat aanschrijven dat toegang tot medische gegevens vanaf 1 juli 2015 niet meer mogelijk zal zijn zonder meervoudige authenticatie. "*Alle nieuwe klanten worden direct verplicht meervoudige authenticatie te gebruiken bij toegang tot medische gegevens.*"

In de brief van 12 september 2014 aan de klanten die VCD bij brief van 3 oktober 2014 (in aanvulling op de zienswijze) aan het CBP heeft doen toekomen staat hierover:
"*Vanaf 1 juli 2015 zal iedereen die toegang heeft tot het medische gedeelte van de Humannet applicatie, naast het invoeren van een wachtwoord, ook moeten inloggen met een token naar keuze.*"

VCD stelt in de brief van 11 september 2014 dat het niet volledig aanwezig zijn van meervoudige authenticatie voor al haar klanten, voor zover dit gaat over medische gegevens, niet automatisch leidt tot de conclusie dat er geen sprake is van 'passende maatregelen'.

4. "*Vereisten van in kaart brengen van beveiligingsrisico's en het nemen van (doorlopende) organisatorische en/of technische maatregelen*".

VCD stelt het volgende: " *Zoals uw college zelf stelt in het concept-rapport wordt er door de open normen niet aangegeven wat wordt verstaan onder 'periodiek' in het kader van het in kaart brengen van beveiligingsrisico's. Uw college stelt vervolgens, niet onderbouwd, dat een uitgebreide audit "minimaal 1 keer per jaar" als passend kan worden gekwalificeerd. Hiermee maakt u van een open norm een keihard criterium waarop uw negatieve beoordeling vervolgens wordt gestoeld.*"
VCD geeft aan dat zij deze redenatie zonder nadere onderbouwing niet goed kan volgen en dat ook andere periodieken (groter dan 1 jaar) of andersoortige testen en maatregelen, "*mede conform het hiervoor uitgehaalde uitspraak van de CRvB, ook als 'passend' worden beschouwd waarbij alle omstandigheden van het geval moeten worden meegewogen*."
Het CBP heeft volgens VCD onvoldoende rekening gehouden met de vele andere maatregelen en oplossingen die VCD in haar producten heeft verwerkt. Tevens stelt VCD dat zij in 2013 wel een audit heeft gehouden, te weten het heronderzoek van [Naam bedrijf], versie 1.0, 25 februari 2013.

VCD stelt "*de conclusie die het CBP trekt in het concept-rapport, dat door beveiligingsoplossingen anders dan een jaarlijkse audit geen gevolg is gegeven aan 'passende maatregelen' conform artikel 13 Wbp, is onjuist.*"

Tevens geeft VCD aan dat het CBP louter vanwege het ontbreken van een schatting van de oplossingstermijn en het tijdelijk introduceren van een nieuw beveiligingsrisico bij het oplossen van meerdere andere, stelt dat niet voldaan is aan de eis van (doorlopende) organisatorische en/ of technische maatregelen. " *Bij deze conclusie lijkt het CBP voorbij te gaan aan het algemeen bekende feit, dat zij eerder wel erkende, dat informatiebeveiliging een dynamisch proces*

is." VCD stelt dat het feit dat bij het oplossen van meerdere beveiligingsrisico's er kortstondig één beveiligingsrisico ([risico]) opnieuw even de kop op stak, onverlet laat dat VCD "*voldoende (doorlopend) organisatorische en technische maatregelen neemt en dat de oplossing voor dit kortstondige probleem gewoon door de naleving van het ISO 27001-protocol is geborgd*."

VCD stelt voorts dat zij reeds bij schrijven van 17 juni 2014 heeft aangegeven dat zij voor Humannet Starter en Humannet Verzuim een iteratief beveiligingsproces heeft opgetuigd, "*wat inhoudt dat een cirkelgang van testen van de beveiliging, oplossen van risico's, testen van oplossingen continu plaatsvindt. Het is zonder nadere onderbouwing onbegrijpelijk hoe het CBP desondanks toch de conclusie meent te kunnen trekken dat er geen sprake zou zijn van (doorlopende) organisatorische en technische maatregelen*."

VCD geeft in de zienswijze aan dat zij is overgegaan tot het sluiten van een abonnement op audits c.q. penetratietesten door [Naam bedrijf]. VCD heeft een kopie van het contract bijgesloten.

Tot slot stelt VCD: "*De conclusie die het CBP trekt in het concept-rapport, dat er niet voldaan is aan de eis van (doorlopende) organisatorische en/of technische maatregelen en daardoor geen gevolg is gegeven aan 'passende maatregelen' conform artikel 13 Wbp, is onjuist*."

VCD stelt dat zij op alternatieve wijze wel 'passende maatregelen' heeft genomen en deze "*alternatieve en – conform jurisprudentie – legitieme bewijzen van 'passende maatregelen*"[…] *in overvloed*" aan het CBP heeft doen toekomen.
Het betreft de (verkort weergegeven) volgende maatregelen:

- [Naam bedrijf] heeft de informatiebeveiliging van de applicatie Verzuim als voldoende beoordeeld in het rapport van 25 februari 2013.
- De programmeurs hebben certificaten gehaald van cursussen gericht op informatiebeveiliging.
- VCD heeft een ISMS ingevoerd, dit ter audit gebracht en hiervoor het certificaat NEN-ISO/ IEC 27001 verleend verkregen.
- De scope van de toetsing van NEN-ISO/ IEC 27001 is bewust een brede/ veelomvattende geweest. VCD heeft bewust voor ISO 27001 gekozen "*omdat dit leidende standaard op het gebied van informatiebeveiliging was en is*."
- VCD is een iteratief informatiebeveiligingstraject opgestart met [Naam bedrijf], " *wat inhoudt dat er niet louter één moment een audit wordt gedaan, maar juist dat er constant en in onderlinge wisselwerking de beveiliging constant wordt verbeterd*".
- VCD heeft meerfactor authenticatie geïmplementeerd in Humannet Verzuim en Starter via de applicatie [Naam software], "*maar nog niet al haar klanten willen dit afnemen ondanks het klemmende advies dat cliënte haar klanten heeft gedaan […]*."
- VCD heeft Intrusion Protection Systeem (IPS) geïnstalleerd "*wat haar in staat stelt om dataverkeer te bekijken en op basis van ingestelde 'rules' (regels) bij bepaald dataverkeer direct actie te ondernemen om bepaalde pogingen van misbruik te voorkomen […]*."
- VCD is ook overgegaan op Intrusion Detection System (IDS) van [Naam bedrijf], dat 24 uur per dag, 7 dagen per week de applicaties monitort. Zodra

er sprake is van een aanval op de applicaties, neemt [Naam bedrijf] hierbij direct binnen enkele minuten contact op om VCD te informeren, zodat VCD direct het beveiligingsrisico in kan schatten en, indien noodzakelijk, direct de benodigde beveiligingsmaatregelen kan nemen.
- Penetratietesten door [Naam bedrijf], [Naam bedrijf], [Naam bedrijf] en [Naam bedrijf].

VCD stelt dat zij voor beide applicaties dankzij het ISMS van ISO 27001 procedureel passende maatregelen heeft ingericht door toegang tot een minimum te beperken en via matrices een volledig beeld erop na te houden welke toegang, waartoe en aan wie is verleend." *Daarbij komt nog de inrichting van de applicaties voor gebruik van meervoudige authenticatie.*"
"*Volgens het door uw college in uw concept-rapport aangehaalde citaat van de ICT-Beveiligingsrichtlijnen voor webapplicaties van het NCSC is dat reeds passend, immers: "B0-12 Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/toegangsbeheer [...].*"

VCD geeft aan dat zij niet kan volgen waarom het CBP louter een jaarlijkse audit benadrukt, die ook plaatsvinden, terwijl het in haar concept-rapport volledig voorbij gaat aan het iteratief beveiligingstraject dat continu in volle gang is.

Voorts stelt VCD in de zienswijze van 11 september: "*Uit de rapporten blijkt dat beide applicaties in huidige toestand, ook zonder meervoudige authenticatie, wél veilig zijn, zelfs voor medische gegevens.* […]."

Concluderend stelt VCD ten aanzien van authenticatie het volgende:
"*Ten aanzien van authenticatie [...] geldt dat het CBP ongemotiveerd technische normen hanteert die niet voor de sector van verzuimbedrijven zijn bedoeld of daarop van toepassing zijn. Desalniettemin zal VCD Humannet haar huidige klanten deze maand nog op de hoogte brengen van het nieuwe beleid inhoudende dat per 1 juli 2015 toegang tot medische gegevens louter nog via meervoudige authenticatie mogelijk is. Voor nieuwe klanten geldt dat per direct.*[…]"

Ten aanzien van technische kwetsbaarheden en het in kaart brengen van beveiligingsrisico's en organisatorische en technische maatregelen "*geldt dat uit alle genomen maatregelen, penetratietesten, audits, certificaten en abonnement met [Naam bedrijf] aan deze vereisten werd en wordt voldaan voor beide applicaties. Het CBP stelt een periode van één audit per jaar als norm, terwijl dat niet uit de regelgeving voortvloeit en ongemotiveerd ook niet te volgen is. Het CBP trekt vervolgens met een vreemde redenering de onjuiste conclusie dat louter vanwege het niet hebben gehouden van een jaarlijkse audit (wat het CBP ten onrechte heeft aangenomen voor Humannet Verzuim) geen doorlopende maatregelen zouden zijn getroffen.* […] *De invulling wat als doorlopend moet worden beschouwd is slechts een willekeurige en ongegronde invulling door het CBP.*" VCD merkt op dat zij wel het streven heeft om jaarlijks audits te houden en dat de beide applicaties inmiddels wel doorlopend worden ge-audit, risico's worden continu in kaart gebracht en dat er constant maatregelen worden genomen in software-updates en organisatorisch.

VCD geeft aan dat zij vindt dat het CBP haar conclusie, dat er geen sprake zou zijn van het nemen van 'passende maatregelen' op grond van artikel 13 Wbp, dient te herzien. VCD "*heeft op alternatieve wijzen reeds aangetoond passende maatregelen te hebben*

genomen en te nemen, wat bovendien heeft geleid tot het predicaat 'veilig' voor beide applicaties na de meest recente penetratietesten."

6 DEFINITIEVE BEOORDELING

Het CBP heeft in de voorlopige bevindingen conclusies getrokken ten aanzien van

- Authenticatie bij de toegang tot de applicaties Humannet Starter en Humannet Verzuim waarin medische persoonsgegevens worden verwerkt
- Het periodiek in kaart brengen van technische kwetsbaarheden en het treffen van maatregelen om risico's zoveel mogelijk te beperken.

Authenticatie

Conclusie voorlopige bevindingen
Ten aanzien van authenticatie concludeerde het CBP in de voorlopige bevindingen het volgende.
"*VCD heeft op dit moment nog geen meerfactor authenticatie ingevoerd bij de gebruikers van Humannet Starter en Humannet Verzuim.*[115] *Hiermee voldoen de applicaties Humannet Starter en Humannet Verzuim niet aan de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens*[116]*. Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens zoals bedoeld in artikel 6 Wbp. Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.*"

Zienswijze VCD
Ten aanzien van bovenstaande stelt VCD in de zienswijze van 11 september 2014 samengevat het volgende:

1. De norm die het CBP hiervoor hanteert is ontleend aan beveiligingsstandaarden die niet gelden voor VCD.
2. De applicaties zijn wel veilig, ook zonder meervoudige authenticatie.
3. VCD zal per 1 juli 2015 meervoudige authenticatie toepassen voor de toegang van (arbo)artsen tot de medische gegevens in de applicaties.
4. Het kostenaspect is door het CBP onvoldoende meegewogen.

Ad. 1. De norm die het CBP voor de toegang tot Humannet Starter en Humannet Verzuim hanteert is ontleend aan beveiligingsstandaarden die niet gelden voor VCD.

VCD stelt dat de NEN 7510-norm geen betrekking heeft op bewerkers van verzuimgegevens en door het CBP als onjuiste toetsingsgrond is gebruikt. VCD stelt dat dit blijkt uit de uitspraak van de Centrale Raad van Beroep[117] waarin staat:
"*De NEN 7510 norm is een gezaghebbende sectorale uitwerking van art. 13 Wbp; als een ziekenhuis voldoet aan de NEN 7510 norm, mag ervan uit worden gegaan dat het ook voldoet aan bovengenoemde wettelijke bepaling. Andersom is dit overigens geen volstrekt automatisme: een ziekenhuis kan ook op andere wijze aantonen dat de beveiliging in orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging (ISO 17799).*"
VCD stelt dat uit deze informatie blijkt dat de NEN 7510 norm een sectorale uitwerking is, dus voor zorginstellingen, en derhalve niet zondermeer verbindend is voor VCD.

[115] In de brief van 2 juli van klant 3 is aangegeven dat op dat moment een implementatietraject loopt.
[116] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.
[117] CRvB 1 juli 2008, WBP 2009, afl. 1.

VCD stelt "*De vereenzelviging tussen een zorginstelling en een bewerker van verzuim-gegevens is zonder nadere onderbouwing niet te volgen*."

VCD stelt verder dat het CBP de norm voor betrouwbaarheidsniveau 3 (STORK QAA niveau 3) ontleent aan de "Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten" van Forum Standaardisatie, welke geldt voor elektronische overheidsdiensten, niet voor VCD.
Tevens laat het CBP volgens VCD na te motiveren waarom het STORK-raamwerk als leidend en geldend dient te worden beschouwd, terwijl VCD de Afhankelijkheids- en Kwetsbaarheidsanalyse heeft toegepast in het kader van het ISO 27001-certificeringstraject.
VCD stelt: "*Medische gegevens worden in het kader van niet-zorginstellingen en niet-overheidsdiensten afdoende geborgd door een gedegen informatiebeveiligingsbeleid dat voldoet aan NEN-ISO/IEC 27001*."

Reactie CBP
Het CBP heeft in de voorlopige bevindingen niet gesteld dat de normen voor de zorg en de elektronische overheidsdiensten verbindend zijn voor VCD. De betreffende normen zijn (als voorbeeld) aangehaald omdat deze normen invulling geven aan de open norm van de Wbp ten aanzien van authenticatie bij de toegang tot systemen/ applicaties waarin medische persoonsgegevens worden verwerkt.

De aard van de persoonsgegevens die door VCD in de applicaties Humannet Starter en Humannet Verzuim worden verwerkt, te weten medische gegevens, en de omgeving waarin deze persoonsgegevens worden verwerkt, te weten applicaties waarbij toegang tot de medische gegevens wordt verschaft via internet, zijn zodanig vergelijkbaar met de systemen waar de genoemde normen op toezien, dat niet anders geconcludeerd kan worden dat dezelfde hoge mate van bescherming van toepassing is.

In de voorlopige bevindingen heeft het CBP gesteld dat uit de normen voor de zorg en de elektronische overheidsdiensten voortvloeit dat ten aanzien van authenticatie bij de toegang tot applicaties, die specifiek zijn gericht op het verwerken van medische gegevens en waarbij toegang wordt verschaft via het internet, tenminste gebruik dient te worden gemaakt van tweefactor authenticatie. Zoals bovenstaand uitgelegd heeft dat vooral te maken met het feit dat de applicaties van VCD vergelijkbaar zijn met de systemen waar deze normen op toezien.
Het CBP stelt hiermee derhalve niet dat de normen voor de zorg en voor elektronische overheidsdiensten onverkort van toepassing zijn op VCD.

Zienswijze VCD
VCD stelt dat de NEN 7510 norm enkel te koop is bij NEN en niet publiekelijk vrijelijk beschikbaar en openbaar is en dat het ook op deze grond onjuist is dat het CBP toch deze norm voorschrijft aan cliënte.

Reactie CBP
De NEN 7510 norm is inderdaad niet publiek vrijelijk beschikbaar. De reden hiervoor is als volgt.
De norm NEN 7510 is een door het Nederlands Normalisatie-Instituut (NNI) ontwikkelde norm voor informatiebeveiliging in de zorg die is gebaseerd op de Code

voor Informatiebeveiliging. In een arrest van de Hoge Raad van 22 juni 2012[118] is bepaald dat, nu NEN-normen worden opgesteld door het NNI, een privaatrechtelijke organisatie zonder wetgevende bevoegdheid, de door het NNI opgestelde normen niet als algemeen verbindende voorschriften in de zin van de Grondwet of de Bekendmakingswet kunnen worden aangemerkt. Derhalve behoeven zij niet conform de vereisten van de Bekendmakingswet te worden gepubliceerd in het Staatsblad of de Staatscourant en genieten deze normen auteursrechtelijke bescherming. Dit maakt dat de NEN-normen niet publiekelijk vrijelijk beschikbaar zijn.

Dit neemt echter niet weg dat NEN 7510 richtinggevend is als het gaat om de invulling van artikel 13 Wbp bij verwerkingen van persoonsgegevens in de zorg, of in soortgelijke sectoren. Het feit dat deze norm niet publiekelijk vrijelijk beschikbaar is, doet niet af aan de algemeen erkende maatstaf van beveiliging die uit de NEN 7510 norm voortvloeit.

Zienswijze VCD
Ad. 2. De applicaties zijn wel veilig, ook zonder meervoudige authenticatie.

VCD stelt dat medische gegevens in het kader van niet-zorginstellingen niet-overheidsdiensten afdoende geborgd worden door een gedegen informatiebeveiligingsbeleid dat voldoet aan NEN-ISO/ IEC 27001.

Reactie CBP
Het feit dat VCD een ISO 27001-certificaat heeft, doet niet af aan bovenstaande. Het certificaat houdt in dat het informatiebeveiligingsbeleid dat VCD onderhoudt voldoet aan de eisen van ISO/ IEC 27001:2005. Deze norm is gebaseerd op een procesbenadering van informatiebeveiliging. Het voldoen aan deze norm wil echter niet zeggen dat de beveiliging in de praktijk - in dit geval de toepassing van meervoudige authenticatie bij de toegang tot een systeem waarin medische gegevens worden verwerkt - voldoende is.

Zienswijze VCD
Ook stelt VCD dat, zelfs al zou de NEN 7510-norm zich ook uitstrekken over niet-zorginstellingen, het VCD ook vrij staat om het nemen van 'passende maatregelen' anders aan te tonen. VCD geeft aan dat zij diverse 'passende maatregelen' heeft getroffen zoals:

- [Naam bedrijf] heeft de informatiebeveiliging van de applicatie Verzuim als voldoende beoordeeld in het rapport van 25 februari 2013.
- De programmeurs hebben certificaten gehaald van cursussen gericht op informatiebeveiliging.
- VCD heeft een ISMS ingevoerd, dit ter audit gebracht en hiervoor het certificaat het *certificaat* NEN-ISO/ IEC 27001 verleend verkregen.
- De scope van de toetsing van NEN-ISO/ IEC 27001 is bewust een brede/ veelomvattende geweest. VCD heeft bewust voor ISO 27001 gekozen "*omdat dit leidende standaard op het gebied van informatiebeveiliging was en is*."
- VCD is een iteratief informatiebeveiligingstraject opgestart met [Naam bedrijf], " *wat inhoudt dat er niet louter één moment een audit wordt gedaan, maar*

[118] HR 22-06-2012, ECLI:NL:HR:2012:BW0393

juist dat er constant en in onderlinge wisselwerking de beveiliging constant wordt verbeterd".

- VCD heeft Intrusion Protection Systeem (IPS) geïnstalleerd "*wat haar in staat stelt om dataverkeer te bekijken en op basis van ingestelde 'rules' (regels) bij bepaald dataverkeer direct actie te ondernemen om bepaalde pogingen van misbruik te voorkomen [...].*"
- VCD is ook overgegaan op Intrusion Detection System (IDS) van [Naam bedrijf], dat 24 uur per dag, 7 dagen per week de applicaties monitort. Zodra er sprake is van een aanval op de applicaties, neemt [Naam bedrijf] hierbij direct binnen enkele minuten contact op om VCD te informeren, zodat VCD direct het beveiligingsrisico in kan schatten en, indien noodzakelijk, direct de benodigde beveiligingsmaatregelen kan nemen.
- Penetratietesten door [Naam bedrijf], [Naam bedrijf, [Naam bedrijf] en [Naam bedrijf].

VCD stelt dat zij dankzij het ISMS van ISO 27001 procedureel passende maatregelen heeft ingericht door toegang tot een minimum te beperken, en via matrices een volledig beeld erop na te houden welke toegang, waartoe en aan wie is verleend.

Reactie CBP
VCD verwerkt medische gegevens van zieke werknemers in de applicaties Humannet Starter en Humannet Verzuim. Tot deze applicaties wordt toegang verschaft via internet. Dergelijke systemen vereisen een hoog beveiligingsniveau. Vanwege het feit dat in de applicaties van VCD medische gegevens worden verwerkt en toegang tot de medische gegevens in deze applicaties wordt verschaft middels internet, dient dit plaats te vinden middels meerfactor authenticatie.
VCD kan inderdaad ook andere maatregelen treffen om de toegang tot deze gegevens te beveiligen. Zo kan er bijvoorbeeld voor gekozen worden om geen toegang te geven tot de medische gegevens via internet maar bijvoorbeeld via een privaat toegangspunt[119] waarvan de verbinding niet via het publieke internet verloopt.
VCD heeft er echter voor gekozen om voor de verwerking van de medische gegevens van zieke werknemers applicaties aan te bieden die via internet worden ontsloten. Met deze werkwijze als uitgangspunt geldt dat meerfactor authenticatie vereist is.

De door VCD getroffen bovengenoemde maatregelen om de applicaties te beveiligen zien op andere aspecten van de beveiliging dan die van authenticatie. Deze maatregelen zijn derhalve geen alternatief voor meerfactorauthenticatie. Ook autorisatie (als eenmaal toegang tot de applicatie is verkregen, tot welke gegevens binnen deze applicatie heeft iemand vervolgens toegang) ziet niet op een veiliger toegang van gebruikers tot de applicaties (authenticatie). De maatregelen die VCD heeft getroffen zijn derhalve niet passend en kunnen ook niet passend zijn, nu deze geen passend beschermingsniveau bieden voor het verkrijgen van toegang tot de applicatie.

Zienswijze VCD

[119] Een privaat toegangspunt is een directe beveiligde verbinding tussen het gebruikersapparaat en de netwerkprovider zonder gebruik te maken van het internet. Deze directe verbinding kan zowel via bijv. een adsl-verbinding als een mobiel datanetwerk – een mobiel toegangspunt (APN) - lopen.

VCD heeft voorts aangegeven dat zij meerfactor authenticatie heeft geïmplementeerd in Humannet Verzuim en Starter via de applicatie [Naam applicatie], "*maar nog niet al haar klanten willen dit afnemen* […]."

Reactie CBP
Het gegeven dat niet alle klanten meerfactor authenticatie willen afnemen, betekent dat de klanten die dit niet willen afnemen in strijd handelen met artikel 13 Wbp. Dit doet echter niet af aan het feit dat VCD applicaties beschikbaar stelt en beheert die niet voldoen aan de eis die voortvloeit uit artikel 13 Wbp[120] welke inhoudt dat toegang via internet tot applicaties waarin medische gegevens worden verwerkt, dient plaats te vinden middels meervoudige authenticatie. Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens, zoals bedoeld in artikel 6 Wbp. Omdat het beschikbaar stellen en beheren van applicaties die niet voldoen aan artikel 13 Wbp moet worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD hiermee in strijd met artikel 6 Wbp.

Zienswijze VCD
Ad. 3. VCD zal per 1 juli 2015 meervoudige authenticatie toepassen voor de toegang van (arbo)artsen tot de medische gegevens in de applicaties.

In de zienswijze[121] stelt VCD dat het CBP onvoldoende onderscheid maakt tussen een grotere groep gebruikers (ca. [aantal] personen) die toegang heeft tot niet-medische gegevens, en een veel kleinere groep van (arbo)artsen (zo'n [aantal] personen) die wel toegang krijgen tot medische gegevens.

In de zienswijze[122] stelt VCD tevens: "*Desalniettemin zal VCD Humannet haar huidige klanten deze maand nog op de hoogte brengen van het nieuwe beleid inhoudende dat per 1 juli 2015 toegang tot medische gegevens louter nog via meervoudige authenticatie mogelijk is.* […]"

In de brief aan klanten van 12 september 2014 staat[123]: "*Vanaf 1 juli 2015 zal iedereen die toegang heeft tot het medische gedeelte van de Humannet applicatie, naast het invoeren van een wachtwoord ook* ***moeten*** *inloggen met een token naar keuze.*"

Reactie CBP
VCD geeft aan dat zij alleen meerfactor authenticatie gaat invoeren voor de (arbo)artsen, die toegang hebben tot medische gegevens in de applicaties.
In de applicaties Humannet Starter en Humannet Verzuim worden echter alle gegevens (medische en niet-medische) ontsloten door dezelfde infrastructuur.[124] Dit betekent dat de gehele applicatie dient te voldoen aan de hoge eisen die worden gesteld aan databases waarin medische persoonsgegevens worden verwerkt. Iedereen dient derhalve middels meerfactor authenticatie in te loggen op de applicaties.

[120] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.
[121] Brief van 11 september 2014, punt 1.1.
[122] Brief van 11 september 2014, punt 5.
[123] Bijlage in brief van VCD van 3 oktober 2014 aan het CBP.
[124] E-mail van VCD van 12 november 2014 aan het CBP.

Het gegeven dat de toegang tot de verschillende soorten persoonsgegevens binnen de applicatie wordt geregeld middels autorisatieregels[125] doet daar niet aan af. Immers, zoals hierboven reeds aangegeven, ziet autorisatie op een ander aspect van het beveiligingsbeleid, dan de authenticatie, die zoals reeds betoogd, meervoudig van aard dient te zijn.

Daarnaast is het onderscheid tussen medische en niet-medische gegevens niet te maken door onderscheid te maken tussen de registraties van de (arbo)arts en de registraties van andere personen die kunnen inloggen op de applicaties. Niet alleen in de dossiers van de (arbo)artsen staan medische gegevens, ook in de registraties van andere medewerkers staan medische gegevens. Zo kunnen werkgevers onder andere de volgende medische gegevens in het systeem registreren en/ of inzien[126]:

- 1e verzuimdag[127];
- Verzuimreden/ beperkingen;
- Verwachte duur van het verzuim;
- Verzuimpercentage;
- Zwangerschapsverlof;
- Zwangerschapsgerelateerd verzuim;
- WGA registratie (Werkhervattingsregeling voor gedeeltelijk arbeidsgeschikten);
- SFB historie (Structureel functioneel beperkt) en
- Reden beëindiging: o.a. overleden, ziek uit dienst, beëindigd wegens zwangerschapsverlof.

Ook kan de werkgever documenten inzien die worden aangemaakt voor UWV, zoals bijvoorbeeld de probleemanalyse en het plan van aanpak. In deze documenten staan ook medische gegevens, nl. die medische gegevens die de werkgever mag verwerken in het kader van de re-integratie van zieke werknemers.[128] Dit betreft bijvoorbeeld functionele beperkingen en het percentage arbeidsongeschiktheid van de werknemer.

Voor de casemanagers van de arbodienstverleners geldt eveneens dat zij medische gegevens verwerken. Zij kunnen onder andere de volgende medische gegevens registreren[129]:

- Het tijdstip van de ziekmelding;
- De duur van de ziekmelding;
- Percentage arbeidsongeschiktheid;
- Eventuele vangnetsituaties zoals zwangerschap en arbeidsgehandicaptenstatus;
- Fysieke en psychische beperkingen en mogelijkheden (FML);
- Gegevens over ongevallen en
- Afspraken met medische professionals.

[125] Om te voldoen aan artikel 13 Wbp, dient zowel een zo veilig mogelijke authenticatie als een zo veilig mogelijke autorisatie toegepast te worden.
[126] E-mail van VCD van 17 november 2014 aan het CBP.
[127] Het enkele feit dat een persoon ziek is, is ook een medisch gegeven. Zie 'de zieke werknemer en privacy', 2008, pag.27.
[128] Zie bijvoorbeeld 'de zieke werknemer en privacy', CBP, 2008, pag 75.
[129] E-mail van VCD van 17 november 2014 aan het CBP.

Er is derhalve geen (logische, dan wel fysieke) strikte scheiding aan te brengen tussen medische en niet-medische gegevens in de applicaties Humannet Starter en Humannet Verzuim omdat uit bovenstaande blijkt dat ook niet (arbo)artsen medische gegevens verwerken. Ook hieruit vloeit voort dat meerfactor authenticatie vereist is voor iedereen die toegang heeft tot deze applicaties.

Zienswijze VCD
Ad. 4. Het kostenaspect is door het CBP onvoldoende meegewogen.

VCD stelt dat het CBP voorbij gaat aan het feit "*dat de te nemen maatregelen ook proportioneel dienen te zijn in relatie tot de te maken 'kosten van de tenuitvoerlegging'.*" Dat blijkt volgens VCD niet alleen uit de tekst van artikel 13 Wbp, maar ook uit de tekst op de website van het CBP: *"[...]kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist.* "VCD stelt dat ook de wetgever reeds enige tijd terug heeft geconstateerd en overwogen "*dat absolute beveiliging een utopie is en dat maximale beveiliging niet verlangd kan worden omdat 'het onzinnig is een gulden te beveiligen met een rijksdaalder.'(Kamerstukken II 1989/90, 21 551, nr. 3, p.16.)*"

VCD stelt dat zij dit punt meerdere keren heeft aangedragen maar het punt noch de onderbouwde weerlegging niet terug kan vinden in het rapport voorlopige bevindingen.

Voorts maakt het CBP volgens VCD "*onvoldoende onderscheid tussen een grotere groep gebruikers (ca. [aantal] personen) die toegang heeft tot niet-medische gegevens, en een veel kleinere groep van (arbo)artsen (zo'n [aantal] personen) die wel toegang krijgen tot medische gegevens, terwijl dit aspect ook bij de proportionaliteit van de kosten dient te worden meegewogen*."

Reactie CBP
Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin ze worden gebruikt een grotere bedreiging vormt voor de persoonlijke levenssfeer, worden er zwaardere eisen gesteld aan de beveiliging van gegevens. Medische gegevens behoren in de zin van de Wbp tot de categorie bijzondere persoonsgegevens wat betekent dat hoge eisen gesteld worden aan de beveiliging van de gegevens. In dit geval meerfactor authenticatie bij de toegang van gebruikers tot de applicatie met de medische gegevens.
Het feit dat rekening moet worden gehouden met de kosten van de tenuitvoerlegging, betekent niet dat maatregelen niet hoeven te worden getroffen omdat ze kostbaar zijn. VCD kan uiteraard een afweging maken in de keuze voor de vorm van meerfactorauthenticatie op grond van de kosten, zoals zij heeft gedaan door te kiezen voor meerfactor authenticatie van [Naam software] in plaats van die van [Naam bedrijf], die duurder was.
Het is echter niet zo dat meerfactorauthenticatie niet hoeft te worden ingevoerd of alleen voor een deel van de gebruikers hoeft te worden ingevoerd omdat de kosten te hoog zijn. Aangezien het hier om toegang tot applicaties met medische persoonsgegevens via internet gaat is meerfactorauthenticatie een vereiste.

Zienswijze VCD

VCD stelt dat zij het kostenaspect meerdere keren heeft aangedragen bij het CBP maar dit niet terug kon vinden in de bevindingen. VCD verwijst hierbij naar de brief van 15 januari 2014.

Reactie CBP
In deze brief is over het kostenaspect het volgende door VCD gesteld: "*Het absoluut "dichttimmeren" van een op afstand raadpleegbare software-oplossing is bovendien naar de stand der techniek praktisch en technisch onmogelijk en zou bovendien disproportionele financiële investeringen met zich meebrengen van VCD Humannet en/of haar klanten*."

Aangezien VCD met deze zinsnede niet motiveert welk specifiek aspect van de beveiliging waar het CBP onderzoek naar doet hogere kosten met zich meebrengt dan van VCD verwacht kan worden en VCD tevens niet aantoonbaar maakt waarom de kosten te hoog zijn, is het CBP hier in de voorlopige bevindingen niet nader op ingegaan.

Conclusie authenticatie
Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt. Uit artikel 13 Wbp, in samenhang met de Code voor Informatiebeveiliging en de normen die zijn opgesteld voor de zorg en de elektronische overheidsdiensten, volgt dat het verlenen van toegang via internet tot systemen met medische gegevens, dient plaats te vinden middels meervoudige authenticatie.

VCD heeft op dit moment nog geen meerfactor authenticatie ingevoerd voor alle gebruikers van Humannet Starter en Humannet Verzuim. Uit het onderzoek blijkt tevens dat VCD ook in de toekomst niet voor alle gebruikers meerfactor authenticatie gaat invoeren, maar alleen voor (arbo)artsen.

Aangezien in de applicaties Humannet Starter en Humannet Verzuim alle gegevens (medische en niet-medische) ontsloten worden door dezelfde infrastructuur en niet alleen in de dossiers van de (arbo)artsen medische gegevens staan maar ook in de registraties van andere medewerkers, is voor alle gebruikers meerfactor authenticatie vereist.
De voorgestelde werkwijze is derhalve in strijd met de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens. Er is derhalve geen sprake van een behoorlijke en zorgvuldige verwerking van persoonsgegevens zoals bedoeld in artikel 6 Wbp. Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

Technische kwetsbaarheden

Conclusie voorlopige bevindingen
Ten aanzien van technische kwetsbaarheden concludeerde het CBP in de voorlopige bevindingen het volgende.

Voor Humannet Starter hebben geen periodieke audits plaatsgevonden en is onvoldoende opvolging gegeven aan de kwetsbaarheden die zijn geconstateerd in de audit van 16 mei 2014. Hiermee voldoet de applicatie Humannet Starter niet aan de

vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens.[130] Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens zoals bedoeld in artikel 6 Wbp. Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

Voor Humannet Verzuim hebben geen periodieke audits plaatsgevonden. Hierdoor bestaat geen inzicht in de actuele stand van de risico's en de maatregelen die in dat kader getroffen zouden moeten worden. Hiermee voldoet de applicatie Humannet Verzuim niet aan de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens.[131] Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens, zoals bedoeld in artikel 6 Wbp.
Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

Zienswijze VCD
Ten aanzien van de technische kwetsbaarheden, stelt VCD in de zienswijze van 11 september 2014 samengevat het volgende:

1. Het CBP stelt een periode van één audit per jaar als norm, terwijl dat niet uit de regelgeving voortvloeit en ongemotiveerd ook niet te volgen is.
2. Voor Humannet Verzuim heeft wel degelijk jaarlijks een audit plaatsgevonden.
3. Er zijn doorlopend maatregelen getroffen, ook al heeft er geen jaarlijkse audit plaatsgevonden.
4. Beide applicaties worden inmiddels wel doorlopend ge-audit, risico's worden continu in kaart gebracht en er worden constant maatregelen genomen in software-updates en organisatorisch.

Ad.1. Het CBP stelt een periode van één audit per jaar als norm, terwijl dat niet uit de regelgeving voortvloeit en ongemotiveerd ook niet te volgen is.

VCD stelt het volgende: " *Zoals uw college zelf stelt in het concept-rapport wordt er door de open normen niet aangegeven wat wordt verstaan onder 'periodiek' in het kader van het in kaart brengen van beveiligingsrisico's. Uw college stelt vervolgens, niet onderbouwd, dat een uitgebreide audit "minimaal 1 keer per jaar" als passend kan worden gekwalificeerd. Hiermee maakt u van een open norm een keihard criterium waarop uw negatieve beoordeling vervolgens wordt gestoeld*."
VCD geeft aan dat zij deze redenatie zonder nadere onderbouwing niet goed kan volgen en dat ook andere periodieken (groter dan 1 jaar) of andersoortige testen en maatregelen, "*mede conform het hiervoor aangehaalde uitspraak van de CRvB, ook als 'passend' worden beschouwd waarbij alle omstandigheden van het geval moeten worden meegewogen*."

[130] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.
[131] Aangezien de normadressaat van artikel 13 Wbp de verantwoordelijke is, kan de overtreding van VCD (de bewerker) niet aan dit artikel worden toegerekend.

Reactie CBP
Het CBP heeft in de voorlopige bevindingen het volgende gesteld:
Zoals ook is vermeld in het juridisch kader (hoofdstuk 2) staat in de ICT-Beveiligingsrichtlijnen voor webapplicaties van het NCSC[132] onder andere de beveiligingsrichtlijn dat penetratietesten en audits periodiek moeten worden uitgevoerd.
Hierbij wordt niet aangegeven wat wordt verstaan onder 'periodiek'. Beveiliging is, zoals VCD zelf ook aangeeft, een dynamisch proces waarin dagelijks nieuwe risico's ontstaan. Deze kunnen bijvoorbeeld ontstaan door kwetsbaarheden in nieuwe software, door kwetsbaarheden in verouderde software maar ook doordat er door de beheerder zelf doorlopend aanpassingen aan het systeem/ de applicaties worden gedaan. Doordat er doorlopend nieuwe risico's kunnen ontstaan is het CBP van oordeel dat het passend is om, zeker in het geval van een applicatie waarin medische gegevens worden verwerkt, meerdere penetratietesten/ scans per jaar uit te voeren.[133]

In de voorlopige bevindingen staat dus niet dat de norm is dat er 1 keer per jaar een uitgebreide audit moet plaatsvinden maar dat er, zeker bij een applicatie waarin medische gegevens worden verwerkt, meerdere penetratietesten/ scans per jaar moeten worden uitgevoerd. Het CBP geeft in de voorlopige bevindingen ook aan waarom het noodzakelijk is om deze testen/ scans meerdere keren per jaar uit te voeren, namelijk omdat beveiliging een dynamisch proces is waarin dagelijks nieuwe risico's ontstaan, bijvoorbeeld door kwetsbaarheden in nieuwe software of kwetsbaarheden in verouderde software. Doordat er doorlopend nieuwe risico's kunnen ontstaan is het van belang om zo vaak mogelijk inzicht te verkrijgen in de kwetsbaarheden van de applicaties.

VCD heeft tijdens het onderzoek aangegeven dat zij 1 keer per jaar een uitgebreide audit zou gaan uitvoeren.
Ondanks dat dit betekent dat er dus niet meerdere penetratietesten/ scans per jaar worden uitgevoerd, heeft het CBP in de voorlopige bevindingen gesteld dat met deze jaarlijkse audit door VCD wel zou worden voldaan aan het vereiste dat beveiligingsrisico's periodiek in kaart dienen te worden gebracht. Dit, omdat het een uitgebreide audit betrof, te weten een Black Box en een Grey Box en omdat VCD tevens andere maatregelen had getroffen, zoals IDS en het [soort] Monitoring dat wordt uitgevoerd door [Naam bedrijf].

Het CBP heeft derhalve de invulling van de norm wel degelijk onderbouwd en tevens, conform de uitspraak van de Centrale Raad van Beroep waar VCD naar verwijst, de omstandigheden van het geval meegewogen. Het CBP heeft immers gesteld dat met de jaarlijkse uitgebreide audit die VCD zou gaan uitvoeren wel zou worden voldaan aan het vereiste dat de beveiligingsrisico's periodiek in kaart dienen te worden gebracht, ondanks dat er niet meerdere penetratietesten/ scans per jaar zouden worden uitgevoerd.

Zienswijze VCD
Ad. 2. Voor Humannet Verzuim heeft wel degelijk jaarlijks een audit plaatsgevonden.

[132] Deel 1, januari 2012, pag. 17.
[133] Dit kunnen zowel testen zijn die door externe partijen worden uitgevoerd, of testen die intern worden uitgevoerd.

VCD stelt dat zij in 2013 wel een audit heeft gehouden, te weten het heronderzoek van [Naam bedrijf], versie 1.0, 25 februari 2013.

Zoals blijkt uit het documentbeheer in het rapport (pag. iii) is dit een definitieve versie van het rapport dat op 20-12-2012 is opgesteld en op 21-12-2012 intern is gereviewd. Dit is de definitieve versie van de audit dit heeft plaatsgevonden in 2012. Er is derhalve geen sprake geweest van een nieuwe audit in 2013.

Zienswijze VCD
Ad. 3. Er zijn doorlopend maatregelen getroffen, ook al heeft er geen jaarlijkse audit plaatsgevonden.

Reactie CBP
Het CBP heeft volgens VCD onvoldoende rekening gehouden met de vele andere maatregelen en oplossingen die VCD in haar producten heeft verwerkt.
VCD stelt "*de conclusie die het CBP trekt in het concept-rapport, dat door beveiligingsoplossingen anders dan een jaarlijkse audit geen gevolg is gegeven aan 'passende maatregelen' conform artikel 13 Wbp, is onjuist*."
VCD stelt dat zij op alternatieve wijze wel 'passende maatregelen' heeft genomen en deze "*in overvloed*" aan het CBP heeft doen toekomen. (Zie hiervoor het overzicht in de zienswijze van VCD in hoofdstuk 5).

Reactie CBP
VCD heeft lopende het onderzoek diverse maatregelen getroffen. Deze zien echter niet op het periodiek in kaart brengen van kwetsbaarheden middels penetratietesten/ scans. Omdat niet periodiek, bijvoorbeeld tenminste 1 keer per jaar de uitgebreide audit daadwerkelijk plaatsvond, en ook buiten deze audit om geen pentesten/ scans zijn uitgevoerd, heeft het CBP in de voorlopige bevindingen geconstateerd dat door VCD niet is voldaan aan de eis dat de risico's periodiek in kaart worden gebracht middels penetratietesten/ scans.

Zienswijze VCD
VCD geeft aan dat zij niet kan volgen waarom het CBP louter een jaarlijkse audit benadrukt terwijl het in haar concept-rapport volledig voorbij gaat aan het iteratief beveiligingstraject dat continu in volle gang is.
VCD stelt dat zij reeds bij schrijven van 17 juni 2014 heeft aangegeven dat zij voor Humannet Starter en Humannet Verzuim een iteratief beveiligingsproces heeft opgetuigd, "*wat inhoudt dat een cirkelgang van testen van de beveiliging, oplossen van risico's, testen van oplossingen continu plaatsvindt. Het is zonder nadere onderbouwing onbegrijpelijk hoe het CBP desondanks toch de conclusie meent te kunnen trekken dat er geen sprake zou zijn van (doorlopende) organisatorische en technische maatregelen*."

Reactie CBP
Bij het schrijven van 17 juni 2014 heeft VCD ten aanzien van dit onderwerp aangegeven "*Ook de ondersteuning door een partij als [Naam bedrijf] en het iteratieve beveiligingsproces dat in samenspraak met [Naam bedrijf] is ingesteld, tonen het nemen van "passende maatregelen*"."[134]

[134] Brief van VCD van 17 juni 2014 aan het CBP, pagina 4.

Uit deze zinsnede blijkt niet dat er vanaf dat moment daadwerkelijk in de praktijk periodiek penetratietesten/ scans plaatsvinden, noch met welke frequentie deze plaatsvinden.
Het gegeven dat VCD diverse maatregelen heeft getroffen ten aanzien van de beveiliging van de applicaties Humannet Starter en Humannet Verzuim doet niet af aan de constatering dat VCD de beveiligingsrisico's niet periodiek in kaart heeft gebracht.

Zienswijze VCD
Ad. 4. Beide applicaties worden inmiddels wel doorlopend ge-audit, risico's worden continu in kaart gebracht en er worden constant maatregelen genomen in software-updates en organisatorisch.

Reactie CBP
In de zienswijze van 11 september heeft VCD aangegeven dat zij is overgegaan tot het sluiten van een abonnement op audits c.q. penetratietesten. Het contract hiervan is bijgesloten bij de zienswijze van VCD.
Het CBP concludeert derhalve dat VCD op dit moment wel periodiek kwetsbaarheden in kaart brengt middels penetratietesten/ scans.

Zienswijze VCD
VCD stelt in de zienswijze dat het CBP louter vanwege het ontbreken van een schatting van de oplossingstermijn en het tijdelijk introduceren van een nieuw beveiligingsrisico bij het oplossen van meerdere andere, stelt dat niet voldaan is aan de eis van (doorlopende) organisatorische en/ of technische maatregelen. " *Bij deze conclusie lijkt het CBP voorbij te gaan aan het algemeen bekende feit, dat zij eerder wel erkende, dat informatiebeveiliging een dynamisch proces is*." VCD stelt dat het feit dat bij het oplossen van meerdere beveiligingsrisico's er kortstondig één beveiligingsrisico ([risico]) opnieuw even de kop op stak, onverlet laat dat VCD "*voldoende (doorlopend) organisatorische en technische maatregelen neemt en dat de oplossing voor dit kortstondige probleem gewoon door de naleving van het ISO 27001-protocol is geborgd*."

Reactie CBP
Ten aanzien van de tussentijdse rapportage (penetratietest Humannet Starter) van 16 mei 2014) die het CBP van VCD heeft ontvangen voorafgaand aan het uitbrengen van de voorlopige bevindingen is in de voorlopige bevindingen door het CBP het volgende gesteld.
"*Ondanks deze door VCD getroffen maatregelen blijkt uit de penetratietest van 16 mei 2014 dat ook nu weer gebruik kan worden gemaakt van [risico], wat, in combinatie met [risico] en [risico], een risico vormt op ongeautoriseerde toegang tot Humannet Starter. Risico's dienen te worden geïnterpreteerd in de context van het systeem. Omdat in Humannet Starter medische gegevens worden verwerkt, is dit risico onacceptabel.*
Aan de geconstateerde kwetsbaarheid is in ieder geval tot het moment van de brief van VCD aan het CBP van 17 juni 2014 onvoldoende adequate opvolging gegeven. De kwetsbaarheid is nog niet opgelost. Het is voorts niet duidelijk of de kwetsbaarheid op de voorgestelde manier kan worden opgelost[135] *en of er alternatieven zijn. Ook is geen tijdspad aangegeven waarin de kwetsbaarheid zal worden opgelost*."

[135] Het feit dat VCD voor de voorgestelde oplossing afhankelijk is van een externe partij, maakt het risico groter omdat VCD minder invloed heeft.

Het ISO 27001-certificaat van VCD ziet erop toe dat het informatiebeveiligingsbeleid dat VCD onderhoudt voldoet aan de eisen van ISO/ IEC 27001:2005. Deze norm is gebaseerd op een procesbenadering van informatiebeveiliging. Het voldoen aan deze norm wil echter niet zeggen dat de beveiliging in de praktijk - in dit geval het zo adequaat mogelijk opvolging geven aan een geconstateerde kwetsbaarheid - voldoende is.
In bovengenoemde situatie achtte het CBP de opvolging niet voldoende aangezien de kwetsbaarheid nog niet was opgelost en het voorts niet duidelijk was of de kwetsbaarheid op de voorgestelde manier wel kon worden opgelost[136]. Ook waren geen alternatieven bedacht noch was er een tijdspad aangegeven waarin de kwetsbaarheid zou worden opgelost.

VCD heeft met de zienswijze eveneens de meest recente penetratietesten van Humannet Starter[137] en Humannet Verzuim[138] aan het CBP doen toekomen. Deze penetratietesten zien toe op de effectiviteit van de beveiliging van de website, webapplicaties en/ of webservices van Humannet Starter en Humannet Verzuim.

Uit de recente penetratietest van Humannet Starter blijkt dat bovengenoemde kwetsbaarheid inmiddels is opgelost.
De overige uitkomsten van de penetratietesten van Humannet Starter en Humannet Verzuim en de opvolging die aan geconstateerde kwetsbaarheden is en wordt gegeven door VCD, voldoen aan hetgeen verwacht kan worden van VCD om een passend beveiligingsniveau te garanderen ten aanzien van applicaties waarin medische gegevens worden verwerkt.

Op grond van bovenstaande concludeert het CBP dat VCD heeft aangetoond dat zij op dit moment daadwerkelijk een iteratief op risicomanagement gebaseerd beheer van tekortkomingen in de beveiliging van de applicaties Humannet Starter en Humannet Verzuim toepast.

Conclusie technische kwetsbaarheden
Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt. Uit artikel 13 Wbp, in samenhang met de richtsnoeren beveiliging persoonsgegeven, de Code voor Informatiebeveiliging en de ICT-Beveiligingsrichtlijnen voor webapplicaties, volgt dat beveiligingsrisico's periodiek in kaart dienen te worden gebracht, bijvoorbeeld middels penetratietesten en/ of security scans. Daarnaast moeten passende (organisatorische en/ of technische) maatregelen worden getroffen om risico's te beperken danwel te voorkomen.

VCD heeft diverse maatregelen getroffen en heeft aangetoond dat zij op dit moment een iteratief op risicomanagement gebaseerd beheer van tekortkomingen in de beveiliging van de applicaties Humannet Starter en Humannet Verzuim toepast.
De beveiligingsrisico's worden periodiek in kaart gebracht en VCD treft passende maatregelen om risico's te beperken danwel te voorkomen.

[136] Het feit dat VCD voor de voorgestelde oplossing afhankelijk zou zijn van een externe partij, maakte het risico groter omdat VCD daardoor zelf minder invloed had.
[137] Penetratietest Humannet Starter, Rapportage voor VCD, versie 1.1, 29 augustus 2014.
[138] Penetratietest Humannet Verzuim, Rapportage voor VCD, versie 1.2, 29 augustus 2014.

Er is op dit punt derhalve geen sprake meer van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens.

Hiermee handelt VCD, ten aanzien van het in kaart brengen van technische kwetsbaarheden en het treffen van passende (organisatorische en/ of technische) maatregelen om risico's te beperken danwel te voorkomen, op dit moment niet langer in strijd met artikel 6 Wbp.

5 CONCLUSIES

Conclusie authenticatie

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt. Uit artikel 13 Wbp, in samenhang met de Code voor Informatiebeveiliging en de normen die zijn opgesteld voor de zorg en de elektronische overheidsdiensten, volgt dat het verlenen van toegang via internet tot systemen met medische gegevens, dient plaats te vinden middels meervoudige authenticatie.
Aangezien in de applicaties Humannet Starter en Humannet Verzuim alle gegevens (medische en niet-medische) ontsloten worden door dezelfde infrastructuur en niet alleen in de dossiers van de (arbo)artsen medische gegevens staan maar ook in de registraties van andere medewerkers, is voor alle gebruikers meerfactor authenticatie vereist.

VCD heeft op dit moment nog geen meerfactor authenticatie ingevoerd voor alle gebruikers van Humannet Starter en Humannet Verzuim. Uit het onderzoek blijkt tevens dat VCD ook in de nabije toekomst niet voor alle gebruikers meerfactor authenticatie gaat invoeren, maar alleen voor (arbo)artsen.
Deze werkwijze is in strijd met de vereisten zoals die volgen uit artikel 13 Wbp ten aanzien van de beveiliging van de verwerking van (medische) persoonsgegevens. Er is derhalve sprake van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens, wat in strijd is met artikel 6 Wbp. Omdat de tekortkomingen in de beveiliging rechtstreeks moeten worden toegeschreven aan het handelen c.q. nalaten van VCD, handelt VCD in strijd met artikel 6 Wbp.

Conclusie technische kwetsbaarheden Humannet Starter en Humannet Verzuim

Artikel 6 Wbp bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt. Uit artikel 13 Wbp, in samenhang met de richtsnoeren beveiliging persoonsgegeven, de Code voor Informatiebeveiliging en de ICT-Beveiligingsrichtlijnen voor webapplicaties, volgt dat beveiligingsrisico's periodiek in kaart dienen te worden gebracht, bijvoorbeeld middels penetratietesten en/ of security scans. Daarnaast moeten passende (organisatorische en/ of technische) maatregelen worden getroffen om risico's te beperken danwel te voorkomen.

VCD heeft diverse maatregelen getroffen en heeft aangetoond dat zij op dit moment een iteratief op risicomanagement gebaseerd beheer van tekortkomingen in de beveiliging van de applicaties Humannet Starter en Humannet Verzuim toepast.
De beveiligingsrisico's worden periodiek in kaart gebracht en VCD treft passende maatregelen om de geconstateerde risico's te beperken danwel te voorkomen.
Er is op dit punt derhalve geen sprake meer van een onbehoorlijke en onzorgvuldige verwerking van persoonsgegevens.
Hiermee handelt VCD, ten aanzien van het in kaart brengen van technische kwetsbaarheden en het treffen van passende (organisatorische en/ of technische) maatregelen om de geconstateerde risico's te beperken danwel te voorkomen, op dit moment niet langer in strijd met artikel 6 Wbp.