VERTROUWELIJKHEIDSVERSLAG VAN COMNEXIO

INHOUDSOPGAVE

Hoofdstuk I - Inleiding

Ieder jaar sedert 2014 publiceert ORES Assets een vertrouwelijkheidsverslag ter attentie van de CWaPE.
Teneinde te voldoen aan het door de CWaPE aan ORES Assets[1] gerichte verzoek, worden er voor de Groep ORES drie afzonderlijke en specifieke verslagen opgemaakt, namelijk één voor ORES Assets en de twee andere voor elke van haar dochterondernemingen, namelijk ORES cv en Comnexio. Deze drie verslagen worden volgens dezelfde structuur opgemaakt en geven een uitvoerige beschrijving van de goede praktijken die op het vlak van de vertrouwelijkheid worden toegepast. Zij streven ernaar te beantwoorden aan de voorschriften van het decreet waarvan hierna sprake.
Men dient in gedachten te houden dat het operationeel en dagelijks beheer van de activiteiten van ORES Assets[2], met inbegrip van de uitoefening van de strategische en vertrouwelijke taken, enerzijds, en de vertegenwoordiging van ORES Assets in het kader van dat beheer anderzijds, aan ORES cv is toevertrouwd.
Wat de *contact center*-activiteiten betreft, deze werden vanaf 1 juni 2019 toevertrouwd aan Comnexio.
De wijze waarop deze beheersactiviteiten door voornoemde filialen worden uitgeoefend, wordt bepaald in de bijlagen 6 en 7 van de statuten van ORES Assets en door de Raad van Bestuur voor elke bijkomende beslissing.

Het artikel 17 van het besluit van 21 maart 2002 betreffende de netbeheerders, zoals gewijzigd door het besluit van 6 december 2018, bepaalt: "*De netbeheerder zorgt ervoor dat de persoonlijke en commerciële gegevens waarover hij beschikt om zijn taken uit te oefenen, zodanig ingezameld worden dat ze vertrouwelijk blijven. Hij zorgt ervoor dat die gegevens systematisch gescheiden worden van de gegevens die vatbaar zijn voor publiciteit.*"

Het artikel 7 van het besluit van 16 oktober 2003 betreffende de gasnetbeheerders, zoals gewijzigd door het besluit van 6 december 2018 bevat identieke bepalingen.

Sedert de invoering van de inventaris van goede praktijken inzake vertrouwelijkheid, in 2019 door de CWaPE opgesteld in het kader van zijn controle van de bestuursvoorschriften binnen de DNB's en hun dochterondernemingen, tonen die DNB's en hun dochterondernemingen in hun vertrouwelijkheidsverslag aan dat al deze goede praktijken daadwerkelijk werden toegepast.

Onderhavig verslag dekt de activiteiten in 2020 van Comnexio als dochteronderneming van ORES Assets belast met de uitoefening van de taken van *contact center* van ORES Assets sedert 1 juni 2019.

Dit verslag werd goedgekeurd door het Ethisch Comité van Comnexio dat – gezien de gezondheidssituatie en – overeenkomstig de voorschriften van het decreet van 14 januari 2021 tot organisatie, tot en met 31 december 2020, van de vergaderingen van de organen van de intercommunales, van de maatschappijen met een significante lokale

[1] Voorlopige conclusies van de controle op het vlak van de implementering van de bestuursvoorschriften, schrijven van de CWaPE van 15 oktober 2019.
[2] Artikel 13 van de statuten van ORES Assets (zie ook bijlage 6: modaliteiten van de operationele en dagelijkse uitbating verwezenlijkt door de exploitatievennootschap ORES).

overheidsparticipatie, tegelijkertijd fysiek en via videoconferentie werd gehouden met behulp van de TEAMS-applicatie op 24 maart 2021.

Vooraf dient eraan herinnerd te worden dat Comnexio, teneinde op 1 juni 2019 operationeel te zijn, de volgende belangrijkste dienstverleningscontracten heeft gesloten:

- een contract inzake overgangsdiensten met N-Allo. Deze overeenkomst heeft tot doel de overgangsdiensten die door N-Allo aan Comnexio verleend moeten worden te definiëren; en
- een contract inzake ondersteuningsdienstverlening met ORES cv, met name betreffende de basis-IT-diensten.

Tot slot merken we nog op dat Comnexio haar activiteiten van *contact center* enkel voor ORES Assets uitoefent.

Hoofdstuk II – Verplichtingen van het personeel en van de leden van de bestuursorganen inzake de vertrouwelijkheid van de gegevens

1. Verplichtingen van het personeel inzake de vertrouwelijkheid van de gegevens

De type-arbeidscontracten van de personeelsleden bevatten bedingen die hun een verplichting tot vertrouwelijkheid opleggen.
Zo verbinden de personeelsleden er zich met name toe de vertrouwelijke gegevens niet openbaar te maken, deze uitsluitend in het kader van de uitvoering van hun arbeidscontract te gebruiken, deze niet te kopiëren of te reproduceren zonder voorafgaande uitdrukkelijke schriftelijke toestemming van Comnexio, de gegevens die op het ogenblik van de beëindiging van het arbeidscontract nog in hun bezit zijn aan Comnexio terug te geven en dit onmiddellijk na de beëindiging van het arbeidscontract.

Ingevolge de inwerkingtreding van de Algemene Verordening Gegevensbescherming (hierna "AVG"), levert Comnexio een permanente inspanning om de principes van de verordening toe te passen en het personeel te sensibiliseren.
In de loop van het tweede semester 2020 werden de gehele hiërarchische lijn en het ondersteuningspersoneel gesensibiliseerd voor de AVG door de afgevaardigde voor gegevensbescherming (afgekort "DPO" voor "*Data Protection Officer*"). Deze medewerkers kunnen aldus de DPO bijstaan op het terrein.
Bovendien werd er een intranetpagina, die voor alle medewerkers van Comnexio toegankelijk is, aan computerbeveiliging en de AVG gewijd.

Wat de bescherming van de vertrouwelijkheid van de gegevens betreft, omvatten de genomen maatregelen:

- het opleggen van een aantal verplichtingen inzake vertrouwelijkheid via het arbeidsreglement;
- de terbeschikkingstelling van een *Welcome Pack* dat een luik cyberveiligheid bevat aan elke medewerker bij zijn aankomst;
- de terbeschikkingstelling van een korte video die het belang van de veiligheid en de rol die elke medewerker daarbij moet spelen toelicht;
  een *e-learning*-module "AVG" en diverse *e-learning*-modules betreffende informatiebeveiliging werden in 2020 uitgewerkt voor alle medewerkers. Vervolgens worden deze boodschappen sedert eind 2020 en op een permanente wijze beklemtoond via bewustmakingscampagnes over diverse veiligheidsonderwerpen, afhankelijk van de kennis die bij de medewerkers wordt vastgesteld en de belangrijkste bedreigingen waaraan onze gegevens zijn blootgesteld.

Ter herinnering, de bovenstaande informatie maakte reeds het voorwerp uit van een verslag van de CWaPE in het kader van haar controle op de implementering van de bestuursvoorschriften.

2. Verplichtingen van de leden van de bestuursorganen inzake de vertrouwelijkheid van de gegevens

Naast de algemene plicht tot terughoudendheid die op elke bestuurder van een vennootschap rust, worden de bestuurders van Comnexio bewust gemaakt van hun vertrouwelijkheidsplicht via de bestuursvoorschriften die in haar schoot zijn aangenomen en toegepast (in casu het “Bestuurscharter van het bedrijf”, dat trouwens toegankelijk is op de website).

Zij hebben er zich eveneens individueel toe verbonden, met name, de deontologische regels na te leven, in het bijzonder op het vlak van belangenconflicten, het gebruik van voorwetenschap, loyauteit, discretie en goed beheer van overheidsmiddelen, overeenkomstig het artikel L1532-1, § 1, van het Wetboek van de Lokale Democratie en de Decentralisatie, en dit door het ondertekenen van een verklaring op eer in dat verband.

Hoofdstuk III – Beveiligingsmaatregelen betreffende de toegang van het personeel tot persoons- en commerciële gegevens

Wanneer Comnexio persoonsgegevens verwerkt in verband met het cliënteel van ORES, wordt er alles aan gedaan, of het nu is op het vlak van personeel, onderaannemers of computerbeveiliging, om de vertrouwelijkheid van de ter beschikking gestelde persoons- en commerciële gegevens te bewaren. De persoonsgegevens van de netgebruikers die bij diverse gesprekspartners worden ingezameld, beperken zich tot de informatie die noodzakelijk is voor de uitvoering van de taken in verband met de legitieme taken van ORES: aansluitingen, geplande werken tellingen, ODV,…

Zowel ORES als Comnexio voerden reeds in de ontwerpfase ("*Privacy by design"*) beschermingsprocedures in op zodanige wijze dat er van bij het opstarten van nieuwe projecten of ter gelegenheid van wijzigingen van de bestaande verwerkingen rekening wordt gehouden met de aspecten betreffende de persoonsgegevens van haar klanten.

Tegelijkertijd heeft Comnexio begin 2020 oefeningen opgestart in verband met het bijwerken van haar verwerkingsregister en de DPIA "*Data Protection Impact Assessments"* (hierna "DPIA") met het oog op het analyseren en evalueren van de risico's verbonden aan gegevensverwerkingen die reeds voor de inwerkintreding van de AVG bestonden en het voorzien van een plan om daaraan te verhelpen. Het aspect "toegang" tot de persoonsgegevens wordt in deze oefeningen geëvalueerd.
Bovendien schrijft een procedure, die momenteel wordt uitgeschreven, voor dat dergelijke DPIA moeten worden uitgevoerd voor elke nieuwe verwerking die zou kunnen "*resulteren in een hoog risico voor de rechten en vrijheden van natuurlijke personen*", die klanten van ORES zijn.

De volgende technische en organisatorische maatregelen worden toegepast:

- Het beheer van de machtigingen voor de computerapplicaties die zowel door ORES als door N-Allo worden gehost is gecentraliseerd en geautomatiseerd met behulp van de tool "*SAP Identity Management"* (bijvoorbeeld: Sap: lopex, procli; *Active directory*: Mercure, Oracle: netgis).
- De methodologie die voor de regeling van de toegangen wordt toegepast is de "op rollen gebaseerde toegangscontrole", waaraan ORES (in de hoedanigheid van IT-dienstverlener van Comnexio) de twee volgende principes toevoegt: "*least privilege"* en "*need to know"*.
- In het geval van geprivilegieerde toegangen, maken deze laatste het voorwerp van een specifiek goedkeuringsproces uit.
- Wat de levenscyclus van de computeridentiteiten betreft, deze wordt automatisch aan het personeelsbeheer aangepast.
- De toegangsrechten tot de computerapplicaties worden beheerd door ORES en in hoofde van Comnexio gevalideeerd door de *service delivery manager*.
- De bestekken betreffende de nieuwe applicaties vermelden specifiek de behoefte tot integratie in het systeem voor het beheer van de computeridentiteiten en -toegangen dat door ORES cv werd ingevoerd (in de hoedanigheid van IT-dienstverlener van Comnexio).

In verband met de Koepel[3] dient het volgende te worden opgemerkt:

- De doorgang via de Koepel stelt Comnexio in staat, enerzijds, tot het filteren van de toegang tot de klanteninformatie en, anderzijds, tot het filteren van datgene waartoe de klantenadviseurs, eens dat zij verbonden zijn, toegang kunnen krijgen;
- Voor het geval van het vertrek van een personeelslid van Comnexio of van een vervanging, werd er een spoedprocedure ingevoerd. De toegangen worden, afhankelijk van het geval, ingetrokken of toegestaan;
- Het personeel van Comnexio beschikt over een *login* via een ORES-werkstation op een door ORES beheerd netwerk.

[3] Sedert 31 december 2020 gebruikt Comnexio de N-Allo-koepel niet meer. Deze werd vervangen door een door ORES ontwikkelde applicatie. De ORES-koepel is een interface die de verwerking van de interacties (identificatie van de klant en automatisering van de meteropnameprocessen) vergemakkelijkt voor de klantenadviseurs van Comnexio en het traceren van de redenen van de oproepen mogelijk maakt.

Hoofdstuk IV – Beveiligingsmaatrelen in verband met de toegang van de leveranciers en de klanten tot de vertrouwelijke gegevens

Comnexio heeft toegang tot de informatie van het toegangsregister of nog van Mercure om de eerstelijnsoproepen van de klanten te beantwoorden.

Het beheer van de toegang tot de applicaties door Comnexio en de manier waarop de informatie aan de klanten wordt meegedeeld, worden in het volgend punt uitgelegd.

Specifieke maatregelen

- *Het toegangsregister*

  De computerinfrastructuur is beveiligd en de toegang tot de applicatie is voorbehouden.
  Elke nieuwe aanvraag tot toegang wordt overgemaakt aan ORES, die deze volgens haar interne procedure goedkeurt. Voor het overige verwijzen wij naar de verslagen die voor ORES Assets en ORES cv werden opgesteld.

  De procedure die binnen Comnexio wordt toegepast wordt beheerst.
  De klantenadviseurs geven via de telefoon, per brief of per mail enkel inlichtingen door aan de klant (of aan een door hem gemachtigde persoon) die op het toegangspunt erkend is en enkel gedurende de periode van bewoning van deze klant. Er zal hem gevraagd worden zijn meternummer voor controle mede te delen.
  Als een klant aan de DNB vraagt welke leverancier aan het toegangspunt verbonden is, zal die informatie hem per brief naar het installatieadres worden gestuurd.
  Derhalve, als de aanvraag uitgaat van een commerciële leverancier, zal hij automatisch naar het toegangsregister (*supplier web*) verwezen worden, gezien de toegangen waarover hij beschikt.
  Als het om een klant gaat, zal hem zijn EAN enkel kunnen worden meegedeeld op voorwaarde dat hij zijn meternummer opgeeft. Als de klant zijn meternummer niet kan opgeven, zal de EAN niet telefonisch aan hem kunnen worden meegedeeld, maar zal deze hem per brief naar het verbruiksadres gezonden worden. Als het gaat om een aanvraag betreffende meer dan twee EAN-codes, dan zal aan de klant gevraagd worden zijn aanvraag per brief of per e-mail, samen met de lijst van de betrokken adressen en meternummers, te sturen.
  Deze oproepen en berichten zullen in de Koepel nagetrokken worden.

  Er dient te worden opgemerkt dat er binnen ORES in samenwerking met Comnexio een verbeteringstraject loopt in verband met de aanvragen “uw EAN kennen” teneinde deze informatie slechts aan een enkele klant die op het toegangspunt actief is mee te delen.

  Comnexio verstrekt ook klanteninformatie aan de OCMW’s. Het OCMW beschikt over een specifiek contactnummer om informatie op te vragen in verband met zijn bestuurden (staat van een dossier, leverancier actief op een punt,

verbruikshistoriek, …) voor wie het over een permanent mandaat beschikt. Aan de OCMW's wordt gevraagd dit oproepnummer nooit openbaar te maken.

- *Mercure-systeem*

  De computerinfrastructuur is beveiligd en de toegang tot de applicatie is geïndividualiseerd en voorbehouden in de "wijzigings-"modus aan het personeel van Comnexio, maar enkel via een met een paswoord beveiligde webinterface (*Measure Web)*.

  Voor het overige verwijzen wij naar de verslagen opgesteld voor ORES Assets en ORES cv.

  De procedure die binnen Comnexio wordt toegepast wordt beheerst.
  De klantenadviseurs geven via de telefoon, per brief of per mail enkel inlichtingen door aan de klant (of aan een door hem gemachtigde persoon) die via zijn EAN herkend wordt en enkel gedurende de periode van bewoning van deze klant. Er zal hem gevraagd worden zijn meternummer voor controle mede te delen.
  Als de klant opbelt om zijn verbruikshistoriek te kennen, zal hem volgens de geldende procedure het volgende worden meegedeeld::
  - Als het om een opname vanop afstand gaat (buiten de communicerende meter), moet men de klant verzoeken zijn aanvraag via de website van ORES in te dienen. Hij ontvangt dan een historiek over de drie laatste jaren maximum.
  - Als het om een jaarlijkse of maandelijkse opname gaat, worden de klantenadviseurs er eerst aan herinnerd dat de verbruiksgegevens privé-inlichtingen zijn. Als een eigenaar het verbruik van zijn huurders wenst te kennen, moet hij dat rechtstreeks aan zijn huurders vragen.

- *Registratie*

  De communicaties tussen de klantenadviseurs van Comnexio en de gesprekspartners worden met naleving van de voorschriften van de wet inzake elektronische communicatie geregistreerd. Op die manier, in het kader van het hiervoor bedoelde overgangscontract tussen N-Allo en Comnexio en op verzoek van deze laatste, verzamelt en registreert N-Allo elektronische communicaties en de gegevens die daarin worden uitgewisseld (calls, e-mails, chats...) en uitgaan van de klantenadviseurs van Comnexio. Tot slot, hoewel het N-Allo-platform de registratie van de interacties tussen de klanten en de klantenadviseurs van Comnexio mogelijk maakt, kan uitsluitend het personeel van Comnexio over deze registraties, die zijn opgenomen in aan Comnexio voorbehouden directory's, beschikken.

  Standaard worden deze registraties bewaard gedurende een maand vanaf de datum van de communicatie. Voor de registraties die krachtens de wettelijke verplichtingen gebeurden wordt evenwel een regelmatige extractie voorzien met het oog op de bewaring door Comnexio.

Hoofdstuk V – Beveiligingsmaatregelen betreffende de toegang van de onderaannemers tot de vertrouwelijke gegevens

Contractuele maatregelen

Bij het sluiten van transacties of contracten met haar partners, worden daarin systematisch “AVG”-bedingen ingevoegd. Deze preciseren alle in het artikel 28 van de AVG voorziene elementen: duur, toepassingsgebied, finaliteit, verwerkingsinstructies, voorafgaande toestemming in het geval dat er beroep wordt gedaan op een onderaannemer, terbeschikkingstelling van alle documentatie waaruit de conformiteit blijft, onmiddellijke kennisgeving van elke schending van gegevens …

Van zodra er gegevens buiten de Europese Unie worden gedeeld, worden de contractuele typebedingen toegepast.

Er worden eveneens ruimere vertrouwelijkheidsbepalingen in de contracten voorzien.

Specifieke maatregelen

De tussen N-Allo en Comnexio gesloten overgangsovereenkomst legt aan de partijen een door hen na te leven vertrouwelijkheidsverplichting op. Zo verbinden zij er zich met name toe de vertrouwelijkheid van de gegevens te bewaren, deze enkel in het kader van de uitvoering van de overeenkomst te gebruiken, de vertrouwelijkheid van dergelijke gegevens te bewaren en voorzorgsmaatregelen te nemen teneinde deze te beschermen, deze niet aan een derde te onthullen, behoudens schriftelijke voorafgaande toestemming van de andere partij, en de vertrouwelijke gegevens terug te geven of te vernietigen wanneer zij voor de andere partij geen nut meer hebben.

Bovendien, in het kader van de AVG, wanneer N-Allo of Comnexio persoonsgegevens betreffende de klanten van ORES verwerkt, handelt ORES in de hoedanigheid van verwerkingsverantwoordelijke, Comnexio in de hoedanigheid van onderaannemer en N-Allo in de hoedanigheid van onderaannemer in tweede rang krachtens het overgangscontract. Comnexio bemoeit zich enkel met de gegevens van ORES op instructie van deze laatste.

In de praktijk stelt N-Allo een geheel van applicaties ter beschikking van Comnexio, die geen gevoelige gegevens bevatten, zoals het communicatieplatform en de daarmee verbonden applicaties (*call flows*, IVR,…). Deze applicaties bevatten dus slechts een zeer beperkt aantal klantengegevens.
Er dient evenwel te worden opgemerkt dat het communicatieplatform de registratie van interacties tussen de klanten en de klantenadviseurs van Comnexio mogelijk maakt. Wij verwijzen in dat verband naar de ontwikkelingen die in Hoofdstuk IV van onderhavig verslag in verband met de registraties worden behandeld.

Het technisch team dat het beheer van de informatiesystemen verzekert, beschikt in het strikte kader van deze opdracht eveneens over toegangen tot de databanken.

De *reporting*-omgeving bevat enkel beperkte operationele gegevens, die aan de medewerkers van Comnexio gelinkt kunnen worden. Anderzijds bevinden er zich in deze *reporting*-omgeving geen “klanten”-gegevens.

Tot slot is dat ook het geval voor de Nice WFM-applicatie, die de planning van de middelen mogelijk maakt. Zij bevat gegevens over de medewerkers van Comnexio maar geen gegevens over de gebruikers van het netwerk.

IT-diensten

Comnexio heeft alle basis-IT-diensten, zoals de levering, de installatie en de ondersteuning van de werkstations, de *printing,* de internettoegang, het beheer van de *Active Directory*, de toegang tot het netwerk …, aan het IT-Departement van ORES cv toevertrouwd. De betrokkenheid van N-Allo beperkt zich strikt tot het beheer van de tickets (incidenten of *service requests)* met betrekking tot de applicaties die N-Allo ter beschikking van Comnexio stelt. De omvang van de betrokkenheid van N-Allo wordt op strikte wijze contractueel bepaald in de eerder genoemde overeenkomst inzake overgangsdiensten. In de praktijk wordt deze betrokkenheid omkaderd door nauwkeurige procedures en volledig beheerd via het IT-Departement van ORES cv, zonder rechtstreeks contact tussen N-Allo en de medewerkers van Comnexio.

Bij de oprichting van Comnexio werd er een bepaling inzake computerbeveiliging ingevoerd, die ter goedkeuring aan de CWaPE [4] werd voorgelegd. Deze voorziet onder andere:

- een compartimentering op informaticavlak van de systemen en applicaties die door N-Allo ter beschikking van Comnexio worden gesteld (“*Chinese Wall”*), zoals voorzien in de overeenkomst inzake overgangsdiensten tussen Comnexio en N-Allo:
    - N-Allo waarborgt dat de toegangen tot de gegevens van de applicaties die uitsluitend ter beschikking van Comnexio worden gesteld beperkt worden tot enkel de medewerkers van Comnexio en tot het personeel van N-Allo waarvoor de toegang strikt noodzakelijk is voor het verstrekken van de computerdiensten. Deze gegevens worden anderzijds opgeslagen in computeromgevingen die eigen zijn aan Comnexio en volledig gescheiden zijn van de computeromgevingen van de klanten van N-Allo;
    - Comnexio behoudt zich het recht voor over te gaan tot de controles die zij nodig acht om met name de goede compartimentering op informaticavlak van de applicaties die haar door N-Allo ter beschikking worden gesteld te controleren, alsook van de daaraan gelinkte gegevens. Als ingevolge deze controles zou blijken dat N-Allo haar verplichtingen inzake compartimentering niet (meer) nakomt, verbindt N-Allo zich ertoe zich in dat opzicht zo spoedig mogelijk aan te passen;
- een echte scheiding tussen de activiteiten van Comnexio en van N-Allo, zelfs al worden de gebouwen verder gedeeld (fysieke scheiding van de teams).

[4] Aanvraag tot het verkrijgen van de toestemming van de CWaPE van 29/03/2019 met het oog op het toevertrouwen van de *contact center*-activiteiten aan een nieuwe dochteronderneming van ORES Assets.

Hoofdstuk VI – Traceerbaarheid als vector van vertrouwelijkheid

Comnexio delegeert het beheer van zijn IT-dienst aan ORES cv.

Meer bijzonderheden over het beheer van de traceerbaarheid van de toegangen door ORES cv zijn terug te vinden in het vertrouwelijkheidsverslag van ORES cv.

Hoofstuk VII – Het delen van IT-systemen en -infrastructuren met andere bedrijven

De IT-systemen en -infrastructuren van Comnexio worden beheerd door ORES cv krachtens het hiervoor bedoelde contract inzake ondersteuningsdiensten tussen ORES cv en Comnexio. In dat verband is het beheer van de Veiligheid van de informatie het beheer van ORES, dat zich aan de ISO27001-norm confirmeert.
Bijgevolg is de scheiding van de aldus gedeelde gegevens gebaseerd op de volgende principes:

- het “minste voorrecht” (“*least privilege”*): aan een gebruiker moeten standaard enkel de toegangsrechten worden toegekend die strikt noodzakelijk zijn voor de uitvoering van zijn taak;
- de “scheiding van de taken” (“*segregation of duties”*): de volledige controle op/toegang tot het geheel van een kritisch/gevoelig proces mag niet in handen van één enkele persoon zijn;
- de “noodzaak tot kennisname” (“*need to know”*): een gebruiker mag bepaalde gegevens enkel raadplegen wanneer zijn functie dit werkelijk vereist. Met andere woorden, het feit dat men over een potentiële toegang beschikt om informatie te behandelen volstaat niet om de toegang tot die informatie te rechtvaardigen.

De specifieke maatregelen betreffende N-Allo werden hiervoor behandeld.