Assurance-rapport van de onafhankelijk auditor

Aan	Directie van Stichting ZorgTTP
Opdracht en verantwoordelijkheden	De Autoriteit Persoonsgegevens (AP, voorheen het College Bescherming Persoonsgegevens, CBP) heeft beschreven dat bij toepassing van pseudonimisering geen sprake is van de verwerking van persoonsgegevens, indien aan de volgende voorwaarden is voldaan: 1. Er wordt (vakkundig) gebruikgemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens. 2. Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ('replay back') te voorkomen. 3. Ee verwerkte gegevens zijn niet indirect identificerend. 4. In een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden 1, 2 en 3 is voldaan. 5. De pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt. ZorgTTP is verantwoordelijk voor de volledigheid, het accuraat zijn en de methode van presentatie van de beschrijving (https://www.zorgttp.nl/pages/page/2) en haar managementbewering, het verlenen van diensten die door de beschrijving worden omvat, het vermelden van interne beheersdoelstellingen en het opzetten, implementeren en effectief laten werken van interne beheersmaatregelen om de vermelde interne beheersdoelstellingen te bereiken. Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van een oordeel over de bewering van het management van ZorgTTP over de opzet en werking van interne beheersmaatregelen die verband houden met de interne beheersdoelstellingen die in de beschrijving staan vermeld. Wij hebben bij het vormen van ons oordeel gebruikgemaakt van de criteria die in de navolgende bewering van het management van ZorgTTP staan beschreven en ons onderzoek uitgevoerd om een redelijke mate van zekerheid te verkrijgen dat de beheersmaatregelen van ZorgTTP in opzet en bestaan per 31 december 2015 geschikt zijn om te voldoen aan het normenkader met conformiteitseisen van de toezichthouder "Pseudonimisering van persoonsgegevens" d.d. 25 september 2012 (zie https://www.zorgttp.nl/userfiles/Downloads/Pseudonimisering_van_persoonsgegevens.pdf). Dit verkorte assurance-rapport heeft betrekking op bovenstaande voorwaarden 1, 2 en 3.
Object van onderzoek	De beheersmaatregelen rond de cryptografische systemen en (beheer)processen voor de generieke pseudonimisering van persoonsgegevens. De klantspecifieke processen en maatregelen, alsmede de datacommunicatie tussen ZorgTTP en haar klanten vielen buiten de scope van ons onderzoek.
Werkzaamheden	Wij hebben ons onderzoek uitgevoerd in overeenstemming met het Nederlands recht, waaronder begrepen de Verordening gedragscode en de standaarden en richtlijnen van NBA en NOREA (Richtlijn 3000: Assurance-opdrachten door IT-auditors).
Beperkingen	Ons onderzoek doet geen uitspraak over de juistheid van door ZorgTTP gegeven interpretaties aan en naleving van wet- en regelgeving, zoals de Wet bescherming persoonsgegevens.
Oordeel	Op grond van onze werkzaamheden komen wij tot de conclusie dat het op 31 december 2015 bestaande stelsel van interne beheersmaatregelen in en rondom de pseudonimiseringssoftware en de omringende ICT-beheersomgeving, in voldoende mate in overeenstemming met het gehanteerde 'RAAM'-auditraamwerk zijn vastgelegd en conform de beschreven opzet zijn geïmplementeerd.

Beoogde gebruikers en doel	Deze rapportage is alleen bestemd voor klanten van ZorgTTP die hebben gebruikgemaakt van de pseudonimiseringsdiensten, alsmede voor relevante toezichthouders.

Utrecht, 16 maart 2016
KPMG Advisory N.V.

origineel getekend door

drs. ing. R.F. Koorn RE
Partner

Bewering van het management van Stichting ZorgTTP

De beschrijving en deze bewering zijn opgesteld voor klanten die hebben gebruikgemaakt van het ZorgTTP-pseudonimiseringssysteem en de toezichthouders. Deze doelgroepen worden geacht over voldoende inzicht te beschikken om risico's voortvloeiend uit afwijkingen die van materieel belang zijn in te schatten – in relatie tot de beschrijving van het systeem, samen met overige informatie met inbegrip van informatie over interne beheersmaatregelen die door de klanten zelf worden uitgevoerd.

ZorgTTP bevestigt hierbij dat:

a) de beschrijving van het pseudonimiseringsysteem de gegevensverwerking op 31 december 2015 getrouw weergeeft. De criteria waarvan wordt gebruikgemaakt bij het maken van deze bewering hielden in dat de beschrijving:

   i) weergeeft op welke wijze het systeem is opgezet en geïmplementeerd, met inbegrip van:

      - de soorten diensten die zijn verleend, met inbegrip van, in voorkomend geval de verwerkte persoonsgegevens;
      - de procedures, binnen zowel informatietechnologie als handmatige systemen, waardoor die verwerkingen werden geïnitieerd, uitgevoerd, vastgelegd, gecorrigeerd voor zover noodzakelijk en resulteren in gepseudonimiseerde gegevens en rapportages voor klanten;
      - de verbonden administratie en de ondersteunende informatie waarvan is gebruikgemaakt om verwerking te initiëren, uit te voeren en vast te leggen; dit houdt onder meer in, het corrigeren van incorrecte informatie en op welke wijze informatie over de verwerking van gepseudonimiseerde gegevens is terechtgekomen in rapportages voor klanten;
      - op welke wijze het systeem de significante gebeurtenissen en omstandigheden, buiten de gegevensverwerking, heeft behandeld;
      - het proces waarvan werd gebruikgemaakt bij het verwerken en pseudonimiseren van persoonsgegevens en het opstellen van rapportages voor klanten;
      - relevante interne beheersdoelstellingen en interne beheersmaatregelen die zijn opgezet om die doelstellingen te bereiken;
      - interne beheersmaatregelen waarvan wij, bij de opzet van het pseudonimiseringsysteem, aannamen dat zij door gebruikende klanten zouden worden geïmplementeerd en die, indien noodzakelijk om de interne beheersdoelstellingen die in de bijgaande beschrijving staan vermeld te bereiken, samen met de specifieke interne beheersdoelstellingen die niet alleen door onszelf kunnen worden bereikt, zijn onderkend;
      - overige aspecten van onze beheersomgeving, het risico-inschattingsproces, het informatiesysteem (met inbegrip van het verbonden bedrijfsproces) en communicatie, beheersactiviteiten en interne beheersmaatregelen in het kader van het monitoren die relevant zijn voor het verwerken en pseudonimiseren van persoonsgegevens en het opstellen van rapportages voor klanten;

   ii) geen informatie weglaat of verkeerd voorstelt die relevant is voor de reikwijdte van het systeem dat is beschreven terwijl erkend wordt dat de beschrijving is opgesteld om te voldoen aan de algemene behoeftes van een brede groep gebruikers en hun toezichthouders en daarom niet ieder aspect van het systeem kan bevatten dat iedere individuele cliënt in diens eigen bijzonder omgeving belangrijk kan achten;

b) de interne beheersmaatregelen die verband houden met de normen zoals gesteld door de Autoriteit Persoonsgegevens (voorheen CBP) op afdoende wijze zijn opgezet op 31 december 2015. De voorwaarden zoals gehanteerd tijdens het onderzoek zijn:

- Er wordt (vakkundig) gebruikgemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens.
- Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ('replay back') te voorkomen.
- De verwerkte gegevens zijn niet indirect identificerend.
- De pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.

Wij bevestigen dat ZorgTTP hierbij voldoet aan de criteria in het normenkader met voorgaande conformiteitseisen "Pseudonimisering van persoonsgegevens" d.d. 25 september 2012 (zie https://www.zorgttp.nl/userfiles/Downloads/Pseudonimisering_van_persoonsgegevens.pdf). De criteria waarvan bij het maken van deze bewering werd gebruikgemaakt hielden in dat:

i) de risico's die het bereiken van de beheersdoelstellingen die in de beschrijving staan vermeld in gevaar brengen, werden onderkend; en

ii) de onderkende interne beheersmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de beheersdoelstellingen niet zouden verhinderen.

Houten, 16 maart 2016

origineel getekend door

Drs. J.L. van Vlaanderen
Directeur Stichting ZorgTTP