

AAN Ministerie van VWS

Postbus 20350  
2500 EJ 'S-GRAVENHAGE

DATUM 6 maart 2007

ONS KENMERK z2006-1382

CONTACTPERSOON

UW BRIEF VAN 23 december 2005

UW KENMERK

ONDERWERP pseudonimisering risicoverevening

Geachte ,

In uw brief vraagt u het College bescherming persoonsgegevens (CBP) advies over het toepassen van pseudonimisering van – onder andere medische- persoonsgegevens in het proces van de risicoverevening. De daartoe gekozen aanpak is inmiddels neergelegd in de notitie “Het gebruik van pseudo-identiteiten binnen de risicovereveningssystematiek” door Stichting IVZ (20 juni 2006) – verder te noemen: “de notitie”.

Naar het oordeel van het CBP beschrijft de notitie een correcte toepassing van de pseudonimiseringsooplossing. Daardoor mag redelijkerwijs worden aangenomen dat in het proces van de risicoverevening bij CVZ geen sprake is van verwerking van persoonsgegevens, mits aan een aantal – verder te stellen - voorwaarden is voldaan.

#### *Risicoverevening - doel*

Risicoverevening is de gelijke verdeling van financiële risico's over alle zorgverzekeraars. Door de in de Zorgverzekeringswet opgelegde acceptatieplicht en het verbod om premies te differentiëren naar verzekerdenkenmerken bestaat de kans dat één of enkele verzekeraars een onevenredig groot aantal personen met een hoog gezondheidsrisico moet verzekeren. Om die verzekeraars te compenseren voorziet de Zorgverzekeringswet in risicoverevening.

Gelden van verzekeraars met een klein aantal personen met een hoog gezondheidsrisico worden overgeheveld naar zorgverzekeraars met een groter aantal van die groep. Het geld dat daarvoor nodig is komt uit het Zorgverzekeringsfonds.

Voor het uitvoeren van de risicoverevening is het niet noodzakelijk dat persoonsgegevens worden verwerkt. Wèl is het in de gekozen systematiek nodig dat informatie uit verschillende bronnen kan worden gekoppeld aan één persoon en dat bekend is bij welke zorgverzekeraar hij is verzekerd. Daarbij is het echter niet nodig dat ook bekend is welke persoon hij is.

#### *Gekozen aanpak (op hoofdlijnen)*

De factoren die een rol spelen bij de risicoverevening zijn leeftijd, geslacht, medicijn- en zorggebruik, aard van het inkomen en woonregio.

De gerelateerde gegevens worden betrokken van verzekeraars (leeftijd, geslacht, medicijn- en zorggebruik en woonregio), Belastingdienst (aard van het inkomen, zelfstandigen) en UWV (aard

van het inkomen, uitkeringsgerechtigden), en vervolgens samengevoegd bij het College voor Zorgverzekeringen (CVZ).

Bij de aanlevering van deze informatie worden de identificerende kenmerken van de verzekerde persoon door de verstrekende partij omgezet in een pre-pseudo-identiteit, die in de Trusted Third Party (TTP) nogmaals wordt versleuteld tot een pseudo-identiteit. Bij CVZ zijn alle gegevens die betrekking hebben op deze persoon uitsluitend gekoppeld aan deze pseudo-identiteit. Ook de afnemers van CVZ beschikken – voor zover noodzakelijk - derhalve uitsluitend over een pseudo-identiteit.

#### *De rol van VEKTIS*

In het proces van de risicoverevening zijn de meeste en gevoeligste gegevens afkomstig van de verzekeraars. In de notitie is aangegeven dat deze gegevens mogelijk eerst zullen worden verzameld door VEKTIS, die vervolgens de boven beschreven pre-pseudonimisering uitvoert alvorens de gegevens via de TTP naar CVZ worden verzonden.

Ook overigens speelt VEKTIS in de beschreven opzet een belangrijke rol: VEKTIS is namelijk eveneens "leverancier" van gegevens aan de onderzoeksbureaus en "uitvoerder" van SA-Z. De betrokken verwerkingen bevinden zich buiten het pseudonieme domein en vallen derhalve onder de Wet bescherming persoonsgegevens (WBP).

Het CBP heeft daarom bij brief van 14 december 2006 vragen gesteld aan ZN en VEKTIS in verband met de beoogde rol van VEKTIS. Deze vragen waren met name gericht op het - voor zover mogelijk - uitsluiten van dubbelrollen en indirecte herleidbaarheid en indirect ook op de vaststelling dat VEKTIS een – vanuit het oogpunt bescherming persoonsgegevens - voldoende betrouwbare partij is gezien de haar in dit kader toebedeelde taak.

Deze vragen zijn op 11 januari 2007 beantwoord door ZN. Op enkele punten bleef nog onduidelijkheid bestaan zodat nog aanvullende vragen per e-mail zijn gesteld op 23 januari 2007.

Deze vragen zijn op 1 februari 2007 beantwoord door VEKTIS. Naar het oordeel van het CBP is hiermee voldoende informatie over de verwerkingen bij VEKTIS verkregen om te kunnen vaststellen dat de beoogde rol van VEKTIS niet in de weg hoeft te staan aan een correcte uitwerking van de pseudonimiseringsoplossing.

#### *Beoordeling*

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 sub a WBP). Uitgangspunt is dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Bij toepassing van pseudonimisering is geen sprake van verwerking van persoonsgegevens, indien aan de volgende voorwaarden is voldaan:

a. er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens;

- b. er zijn technische en organisatorische maatregelen genomen om herhaalbaarheid van de versleuteling ("replay attack") te voorkomen;
- c. de verwerkte gegevens zijn niet indirect identificerend, en
- d. in een onafhankelijk deskundig oordeel (audit) wordt vooraf en daarna periodiek vastgesteld dat aan de voorwaarden a, b en c is voldaan.

Deze voorwaarden zijn ook gesteld bij de vormgeving van het DIS. Het CBP heeft zich toen reeds uitgebreid gebogen over de toepassing van pseudonimisering en gaat er bij de beoordeling van het onderhavige rapport van uit dat de voor het DIS geformuleerde uitgangspunten eveneens bij de risicoverevening zullen gelden. Eén van de uitgangspunten is voorts dat de pseudonimiseringsooplossing op heldere en volledige wijze dient te worden beschreven in een actief openbaar gemaakt document zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.

#### *Conclusie*

Naar het oordeel van het CBP mag redelijkerwijs worden aangenomen dat de notitie een correcte uitwerking vormt van de voorwaarden a. en b.

#### *Tenslotte*

Zodra niet (meer) aan de bovengenoemde vier voorwaarden wordt voldaan, is sprake van persoonsgegevens en is de WBP weer onverkort van toepassing ten aanzien van die gegevens. Daarbij kunnen ook technische ontwikkelingen een rol spelen. Wat bij een bepaalde stand van de techniek immers als anoniem, want redelijkerwijs niet tot een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen – bijvoorbeeld op het gebied van de cryptografie - alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding. Nu voor verwerking van persoonsgegevens ten behoeve van de risicoverevening geen rechtsgrond bestaat, zou in dat geval sprake zijn van een onrechtmatige gegevensverwerking. Het blijven voldoen aan de gestelde voorwaarden vereist dus continue inspanning.

De vormgeving van de TTP vormt een belangrijk aandachtspunt in de verdere uitvoering. De onafhankelijkheid, deskundigheid en betrouwbaarheid van de TTP dienen boven elke twijfel verheven te zijn.

Soms leiden gegevens niet direct tot identificatie van een bepaald persoon maar kunnen de gegevens via nadere stappen, bijvoorbeeld door combinatie met andere gegevens, in verband worden gebracht met een bepaalde persoon. In dat geval is sprake van indirect identificerende gegevens.

Bij de verdere uitwerking zal reeds in een vroeg stadium – in de fase systeemontwerp en bij de definitie van de gegevenssets - dienen te worden onderzocht of de verwerkte gegevens niet indirect identificerend zijn. Dit onderzoek dient verderop in de levenscyclus van het risicovereveningssysteem bij wijziging van de gegevenssets en overigens periodiek te worden herhaald.

Een ander aandachtspunt is de toekomstige rol van VEKTIS en met name de levering van persoonsgegevens door VEKTIS aan de zgn. onderzoeksbureaus. VEKTIS kan op dit moment

geen uitsluitel geven of deze gegevensstroom blijft bestaan ook nadat de structurele systeemopzet van de risicoverevening is gerealiseerd.

Het risico bestaat dat deze gegevensstroom de pseudonimisering ondermijnt doordat deze onderzoeksbureaus dan zouden beschikken over zowel identificeerbare als gepseudonimiseerde patiëntgegevens. Dit aandachtspunt dient daarom expliciet te worden geadresseerd bij de verdere uitwerking van de pseudonimiseringsoplossing.

Deze vier punten zijn, naast andere, belangrijke toetsingscriteria bij de uit te voeren audits.

Een kopie van deze brief gaat naar ZN en VEKTIS.

Hoogachtend,

Het College bescherming persoonsgegevens,  
Voor het College,

mw. mr. dr. J. Beuving  
collegelid