Rupsje Nooitgenoeg NZa gaat onder druk een blaadje minder eten

Niet zo prominent was in de nieuwsbrief van de Nederlandse Zorgautoriteit(NZa) op 23 november 2018 te zien dat binnenkort een zeer belangrijke verandering doorgevoerd wordt. De NZa maakte kenbaar dat per 15 april 2019 een wijziging plaats vindt in de inhoud van de Minimale DataSet(MDS) die zorggaanbieders in de specialistische geestelijke gezondheidszorg(GGZ) moeten aanleveren aan het DIS. Dat staat voor het Diagnose Behandel Combinatie(DBC) Informatie Systeem. Daarin slaat de NZa op persoonsniveau gegevens op over medische diagnoses en de behandeling. Ze stelt nu dat na 15 april het aanleveren van de hoofddiagnose volstaat. De informatie over diepere niveaus vraagt men dan niet meer op. Tegelijk meldt de NZa dat informatie over die diepere niveaus die de afgelopen jaren aangeleverd is niet meer voor verdere verwerking beschikbaar zal zijn. **Let wel: hier schrijft de NZA niet dat die dat vernietigd worden, maar dat ze niet meer beschikbaar zijn.** Het is een zeer beperkte aanpassing . Maar deze stap moet wel gezet zijn onder druk van een rechtszaak. Die betreft een eerdere weigering van de Autoriteit Persoonsgegevens om handhavend op te treden tegen de NZa inzake aanlevering van (zeer gedetailleerde) behandelinformatie op persoonsniveau bij het DIS.

Rupsje nooitgenoeg

De NZa geeft met het DIS blijk van een enorme datahonger en is een echt Rupsje Nooitgenoeg. Het zijn data die verzameld worden om beleid te ontwikkelen en ondersteunen in de zorg. Het trieste is dat er bewust voor gekozen is om op persoonsniveau centraal persoonsgegevens te verzamelen. Ook al zijn die gegevens (dubbel) gepseudonimiseerd, het blijven persoonsgegevens. Dat inzicht is de laatste paar jaar steeds duidelijker uitgekristalliseerd en vormt de basis voor verzet tegen het DIS en de ROM-data-verzameling. Voor beleidsontwikkeling en ondersteuning is het totaal onnodig om op persoonsniveau centraal data te verzamelen. Het College Bescherming Persoonsgegevens, de rechtsvoorganger van de Autoriteit Persoonsgegevens, stelde in 2006 al dat een dergelijke dataverzameling tot de zeer risicovolle activiteiten behoort. De hoeveelheid data die de NZa verzameld, vooral in de MDS van de specialistische GGZ is schrikbarend groot. Onder dit artikel heb ik de hele set die de NZa na 15 april 2019 nog wil hebben tegen mijn gewoonte in om een artikel beperkt te houden toch eens afgedrukt. U krijgt dan ook een indruk van de enorme administratieve last die het aanleveren van deze data met zich meebrengt.

Beperking

Wat is nu die beperking die de NZa doorvoert. Binnen de MDS diende de volledige DSM-IV diagnose gespecificeerd te worden. Daarbij gaat het om een psychiatrische diagnose die verpakt is in 5 assen: primaire symptomatologie (de ‘psychische ziekte’), achterliggende persoonlijkheidsstoornissen, (bijkomende) somatische ziekten, psychosociale en uitlokkend factoren en het niveau van functioneren(geschat op een schaal van 1 tot 100). Het behoeft geen betoog dat zoiets een enorm gedetailleerde informatie is over een persoon. Vanaf 15 april 2019 dient alleen de hoofddiagnose, maar niet die van de andere assen aangeleverd te worden.

Rechtszaak

In 2017 diende voor de Rechtbank Midden Nederland de zaak AWB-16_4199 die de burgerrechtenvereniging Vrijbit tegen de Autoriteit Persoonsgegevens(AP) had aangespannen. Als derde partij heeft de NZa ook aan de zitting deelgenomen. De reden was de eis tot handhaving door de AP tegen het verstrekken en verwerken van gegevens door de NZa via het DIS. De meervoudige kamer van de rechtbank deed een tussenuitspraak waarin de AP en NZa de gelegenheid werd geboden om alsnog te voorzien in maatregelen waarmee de gevolgen van de onrechtmatige verwerking van medische persoonsgegevens door het DIS zonder toestemming van de patiënt teniet zouden worden gedaan. De rechtbank deed de uitspraak onder voorzitterschap van mr. Verburg die zich tijdens de zitting uiterst kritisch tegen de AP en de NZa toonde.

Traineren

Uit welingelichte bron vernam ik dat zowel de AP als de NZa er alles aan hebben gedaan om de mediatie te traineren en geen veranderingen in hun handelen aan te brengen. Over de voorzitter van de rechtbank, mr. Verburg, werd in de loop van 2017 bekend dat die benoemd zou worden bij de Raad van State. Het is zeer waarschijnlijk dat het traineren daar deels mee te maken had, omdat men na zijn overstap op een minder kritische rechter hoopt. Daarnaast is het zo dat het handelen van de AP in meer zaken zich kenmerkt door het traineren van beslissingen. Zo wacht een handhavingsverzoek over het door de Stichting Benchmark GGZ verzamelen van ROM-data **al 89 weken** op een beslissing van de AP. De burgerrechtenvereniging is inmiddels het traineren zat. Het gaat voor Vrijbit nu al om 17 maanden na de uitspraak van de rechtbank midden juli 2017. Een nieuwe zitting staat voor februari 2019 op de rol bij de rechtbank.

Eerder vertoond

Al eerder is vertoond dat een data-verzamelende instelling

vlak voor een rechtszitting een aanpassing doet aangaande de gewraakte materie. Zo veranderde de Stichting Benchmark GGZ(SBG) enkele weken voor een rechtszaak van twee patiënten op 13 juli 2017 tegen SBG over ROM-data de wijze waarop een aantal cruciale data aangeleverd dienden te worden. Ook kwam twee dagen voor die rechtszaak de mededeling dat SBG begin 2019 op zou houden te bestaan en op zou gaan in een nieuw op te richten kwaliteitsinstituut voor de GGZ, thans Akwa genaamd. Het is een beproefde tactiek om de beslissing van de rechter te beïnvloeden.

De huidige aanpassing door de NZa past in zo'n rijtje, maar is beslist onvoldoende. Het hele systeem van het DIS waarin op persoonsniveau centraal zorgdata worden verzameld is onnodig voor het doel: beleidsontwikkeling en -ondersteuning in de zorg. Dat kan even goed op basis van geaggregeerde data verkregen met geautomatiseerde rapportages gemaakt op basis van gegevens die (decentraal) bij zorgverleners aanwezig zijn.

W.J. Jongejan, 11 december 2018

12 december: enkele kleine tekstuele aanpasssingen gemaakt in alinea Rechtszaak

---

Minimale dataset vanaf 15 april 2019:

Identificatie zorgaanbieder

Unieke identificatie zorgaanbieder (AGB-code) 1

Patiëntgegevens (gepseudonimiseerd):

-naam cliënt

-geboortedatum

-geslacht

-postcode

-Burgerservicenummer

-unieke identificatie zorgverzekeraar (conform UZOVI-register)

-eerste inschrijfdatum

-laatste uitschrijfdatum

Hoofdbehandelaar

- AGB-code (op persoonsniveau) en diens beroep

Verwijzer

– Het type verwijzer:

1. verwezen patiënt vanuit de eerste lijn (o.a. huisarts, bedrijfsarts)
2. verwezen patiënt vanuit een (andere) ggz-instelling, instelling voor medisch specialistische zorg of ggz-praktijk
3. verwezen patiënt vanuit de crisis zorg of seh.
4. eigen patiënt
5. verwezen patiënt, maar verwijzer heeft geen AGB-code (bijvoorbeeld in geval van een verwijzing naar de crisis zorg, buitenlandse zorgaanbieder, bureau Jeugdzorg)
6. zelfverwijzer
7. bemoeizorg

- AGB-code verwijzer (op persoonsniveau), indien er sprake is van type verwijzer genoemd onder 1 tot en met 4

Productie per cliënt

1. Dbc-trajecten

Dbc:

-zorgtrajectnummer

-begindatum zorgtraject

-einddatum zorgtraject

-circuit

-zorgtype

-DSM diagnoseprofiel op hoofdgroepniveau1

– aantal minuten directe en indirecte patiëntgebonden tijd van iedere hoofdbehandelaar en iedere medebehandelaar en diens beroep

-totaal bestede directe en indirecte patiëntgebonden tijd per dbc

-afspraaknummer/code

Behandeling:

-begindatum dbc-traject

-einddatum dbc-traject

-afsluitreden dbc

-Gedeclareerde prijs

-declaratiedatum

Geleverd zorgprofiel binnen het dbc-traject:

-activiteiten, verrichtingen, overige deelprestaties en producten, zoals gedefinieerd in de Nadere regel gespecialiseerde ggz

-datum + tijdsduur activiteiten/producten

-beroep behandelaar

-deelfactor groepscontacten

Aan structureel onrechtmatige aanmeldingen in LSP moet eind komen

Onlangs kreeg ik zicht op hoe een apotheek op volkomen illegale wijze, volgens de marketingtruc 'ja tenzij' mensen aanmeldt alsof zij toestemming verleend zouden hebben om hun medische gegevens via het Landelijk Schakel Punt(LSP) te laten uitwisselen. De apotheek stopte dit voorjaar hiertoe een brief in de zakjes waarin afgehaalde medicijnen werden meegegeven. Daarin stond aangekondigd dat als men niet voor een bepaalde datum bezwaar aantekende, er na 14 juni 2017 voor hen het LSP zou worden aangezet onder vermelding dat zij door niet te reageren toestemming daarvoor zouden hebben gegeven. Daarnaast werden mensen ook nog eens op onrechtmatige wijze onder druk gezet dat toestemming geven in het belang van hun gezondheid is omdat er zonder aansluiting bij het LSP bijvoorbeeld in de avonduren via een dienstapotheek geen goede medicatie gegeven zou kunnen worden. Heel vilein suggereert het briefje

bovendien dat men alleen maar geen toestemming bij de apotheek zou hebben staan, omdat men de klant al een poos niet aan de balie had gezien vanwege de bezorging van de medicijnen. De apotheek heeft met het sturen van deze brief en het aanmelden van mensen zich onmiskenbaar schuldig gemaakt aan het onder druk zetten van patiënten zodat zij niet in vrijheid zelf kunnen beslissen en aan het gebruik van een wettelijk verboden opt-out-constructie.

Van Gogh-apotheek

De boosdoener is de van Gogh-apotheek in Haarlem. Door op de beschreven wijze medische gegevens van hun klanten open te zetten voor landelijke opvraging door zorgverleners waar betrokkenen geen enkele relatie mee hebben, is bovendien sprake van een grootschalig datalek van uiterst gevoelige medische persoonsgegevens. Omdat VZVZ(beheerder van het LSP) geen uniforme procedure hanteert voor het verkrijgen, registreren en loggen van aangemelde toestemmingen, valt te vrezen dat deze apotheek niet de enige is. Uit onderzoek van Burgerrechtenvereniging Vrijbit, blijkt hoe apotheken, het al dan niet daadwerkelijk verleende toestemmingen verzamelen, organiseren via regionale samenwerkingsverbanden. Volgens de Wet bescherming persoonsgegevens(Wbp) mogen mensen enkel worden aangemeld als zij daarvoor in vrijheid zonder uitoefening van druk en op grond van correcte en heldere informatie ondubbelzinnig toestemming voor hebben verleend.

Bij de doorstart van het LSP is door de voorganger van de huidige Autoriteit Persoonsgegevens(het CBP) op vragen van Nictiz (die het toenmalig door de Eerste Kamer verboden Landelijk Elektronisch PatiëntenDossier(L-EPD)-systeem) over deed aan de private partij VZVZ) duidelijk gesteld dat er sprake moest zijn van de expliciete toestemming van de patiënt via een opt-in systeem.

Geschiedenis

In 2008 had de toenmalige minister van VWS, Ab Klink, bepaald, dat de medische gegevens van iedere burger verplicht beschikbaar werden gesteld voor elektronische uitwisseling via het LSP. Pas toen er grote maatschappelijke onrust ontstond, werd er een uiterst gecompliceerde mogelijkheid aangekondigd waarbij mensen alsnog bezwaar zouden kunnen gaan maken tegen de uitwisseling van hun medische data via het Landelijk Elektronisch PatiëntenDossier(L-EPD). Toen na deze valse start van het L-EPD de Eerste Kamer de hele publieke L-EPD-invoering blokkeerde, werd het concept niet losgelaten, maar zodanig gewijzigd dat er een zogenaamde 'private doorstart' werd gemaakt. Daarbij kwam de verantwoordelijkheid niet langer in handen van de overheidsdienst Nictiz, maar in handen van een private partij. Deze Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ), kreeg het oorspronkelijke systeem onder haar hoede met dien verstande dat de bestaande database gevuld met opt-out-toestemmingen opgeschoond diende te worden.

Acht miljoen mensen werden zo uit de LSP-index verwijderd en alle bezwaren van mensen die aangegeven hadden dat ze niet accepteerde dat hun gegevens via het EPD beschikbaar kwamen werden ongeldig verklaard.(waardoor tot op de dag van vandaag er nog steeds mensen zijn die stellig van mening zijn dat zij expliciet tegen het huidige systeem hebben geprotesteerd omdat zij in 2008, 2009 bezwaar aantekenden).

Opt-in

Cruciaal voor de private doorstart werd geacht dat het geen opt-out (ja tenzij) maar opt-in systeem zou worden. Daarmee werd gesuggereerd dat mensen enkel in het systeem zouden komen als zijzelf daar expliciet toestemming voor gaven. Door deze verschuiving werden en passant alle bezwaren tegen het systeem qua onveilige dataverwerking, het gebruik van het BSN door een partij die daar niet over mag beschikken, en onwettige constructies met betrekking tot de verantwoordelijkheid bij misbruik van medische gegevens en gevraagde generieke

toestemming voor onvoorziene toepassingen, ter zijde geschoven. Feit is dat in 2014 het CBP, na een uiterst beperkt onderzoek(steekproef van 149 personen), al onrechtmatig genoteerde toestemmingen constateerde. Dat werd toen als onbelangrijk incident afgedaan omdat het niet zou gaan om mensen die geen toestemming hadden gegeven maar slechts om administratief niet correct vastgelegde toestemmingen.

Werkwijze apotheek

De brief van de van Gogh-apotheek in Haarlem is gedateerd op 22-05-2017 met als bezwaar-deadline 24-06-2017. De folder van VZVZ die hierbij werd meegestuurd lijkt een poging om de illegale toestemmingsvraag een correct tintje te geven. Maar zelfs die voorlichtingsfolder geeft geen correcte informatie. Deze werkwijze, om via een stilzwijgende opt-out procedure toestemming te veronderstellen en vervolgens te registreren en door te geven aan het LSP voor opname in de verwijsindex, is niet alleen een onrechtmatige handelswijze van de betrokken apotheker, maar maakt ook dat alle aanmeldingen van toestemming vanuit deze apotheek vanaf 14-6-2017 niet langer als rechtmatig kunnen worden beschouwd en uit de verwijsindex verwijderd dienen te worden. Daarnaast is het maar helemaal de vraag of de vreemde opt-out-constructie enkel de mensen treft die de brief bij hun medicijnen meekregen of ook voor alle andere patiënten die bij deze apotheek hun medicatie krijgen, of ook voor de familieleden van de mensen die een dergelijke brief meekregen, maar toevallig geen medicijngebruikers zijn. Vandaar dat alle klanten van deze apotheek geïnformeerd dienen te worden over de onjuiste registratie van ‘toestemming’ alsook over het opvragen van medische gegevens zoals dat heeft plaatsgevonden op basis van de ten onrechte geregistreerde toestemmingen.

Vrijbit

Burgerrechtenvereniging Vrijbit heeft aan de toezichthouder bescherming persoonsgegevens een formeel handhavingsverzoek

gestuurd om hiervoor zorg te dragen. Bovenstaande gang van zaken is één van de methodieken waardoor op illegale wijze toestemmingen vergaard worden door zorgaanbieders. Het gaat met name ook op het landelijk op grote schaal voorkomen van onrechtmatige aanmeldingen door met name de apothekers. Ook hierop ziet het handhavingsverzoek evenals het eerdere handhavingsverzoek wat gebaseerd was op de praktijkvoorbeelden van individuele gevallen waarin mensen ontdekten ten onrechte te staan aangemeld.

VZVZ

VZVZ poogt zich er altijd uit te draaien door te stellen dat zij de toestemmingsvereisten voldoende duidelijk uitleggen in hun folders en voorlichtingsbijeenkomsten. Maar omdat VZVZ een systeem beheert dat onrechtmatig- dan wel helemaal niet verkregen- toestemmingen als grondslag voor aanmeldingen faciliteert, zijn zij uiteraard wel degelijk aansprakelijk. Dit geldt zowel voor het runnen van een systeem waarbij mensen er niet van op aan kunnen dat hun medische gegevens niet ter beschikking worden gesteld aan partijen waar zij geen toestemming voor gaven, als voor de manier waarop de controle hierop systematisch onmogelijk wordt gemaakt. VZVZ voelt wel nattigheid, want in de nieuwsbrief van juli 2017 is een apart stukje aan dit onderwerp besteed. Daarin refereert men aan de recente belangstelling voor verkregen toestemmingen naar aanleiding van de voorbeelden van mensen die onterecht in het systeem bleken te ‘zitten’ en berichtgeving van het tv programma Radar waaruit blijkt dat een substantieel deel van de bevolking geen idee heeft of zij staan aangemeld(en dus wie er over hun medische gegevens kunnen beschikken). Het VZVZ-toestemmingsformulier is inmiddels na jaren zodanig aangepast dat daarop nu wel wordt vermeld dat het over het LSP gaat, maar de informatie blijft te sturend om in vrijheid gegevenstoestemming mogelijk te maken.

Marketing-truc

Aan het op illegale wijze vullen van de LSP-index met vermeende toestemmingen moet een einde komen. Daarbij moet de AP niet schuwen om overtreders aan te pakken voor overtreden van de wet aangaande toestemmingsvereisten en daarmee en het grootschalig en structureel faciliteren van grootschalige datalekken aangaande uiterst gevoelige medische persoonsgegevens. Uiteraard dient ook de hoofdverantwoordelijke VZVZ te worden aangepakt en worden gedwongen om paal en perk te stellen aan de huidige illegale praktijken. Zowel door het verwijderen van (mogelijk) onterechte toestemmingen. Als door het verplicht aanbrengen van systeemwijzigingen waardoor het onmogelijk wordt om onterechte aanmeldingen te *kunnen* doen.

W.J. Jongejan

Plotse verschoning rechter daags voor rechtszaken aantasting beroepsgeheim en privacy

Uit welingelichte bron vernam ik heden dat op donderdag 1 december 2016 één van de rechters van de rechtbank Midden-Nederland bij het bureau wrakingen en verschoningen een

verzoek tot verschoning heeft ingediend. Het betreft de rechter mevr. R.J. Praamstra, die op vrijdag 2 december in een meervoudige kamer met collegae twee zaken zou behandelen. Daardoor gaat de zitting niet door en volgt uitstel. De vereniging Vrijbit spant deze zaken aan tegen de Autoriteit Persoonsgegevens(AP). Het gaat om de zaken met kenmerken UTR 16/3326 en UTR 16/4199. In beide zaken draait het in de kern om de aantasting van het medisch beroepsgeheim en het fundamentele recht van patiënten op bescherming van hun privéleven. Deze zaken hebben zeer duidelijke raakvlakken met het wetsontwerp 33980 dat thans in de Eerste Kamer behandeld wordt. Waar gaat het om? Het gaat om een langlopende kwestie die gaat om de wijze waarop de AP, voorheen het College Bescherming Persoonsgegevens(CBP), haar rol vervult als toezichthouder, ten aanzien van handelen rond medische gegevens. Het lange beloop is voor een groot deel te wijten aan de weigerachtige houding van de AP om op te treden tegen de wijze van handelen van zorgverzekeraars bij het inzien van medische gegevens bij zorgaanbieders.

Zaak UTR 16/3326 WBP V97

Inzet van het geding is de nalatigheid van de toezichthouder Autoriteit Persoonsgegevens om op te treden tegen de wijze waarop de zorgverzekeringsmaatschappijen in Nederland, volgens een gedragscode die in strijd is met zowel de Wet Bescherming persoonsgegevens(Wbp) als het Europees Verdrag voor de Rechten van de Mens (EVRM) verwerkingsprocedures hanteren aangaande de medische gegevens die zij verzamelen en verwerken.

Zaak UTR 16/4199 WBP V93

Inzet van dit geding is het plichtsverzuim van de toezichthouder om op te treden tegen de wijze waarop de Nederlandse Zorgautoriteit (NZa) medische diagnose- en behandelgegevens (DBC) van de gehele Nederlandse bevolking verzamelt, gebruikt en verstrekt aan derden. Namelijk via het

Diagnose-Informatie Systeem (DIS) waar zorgverleners verplicht de DBC-gegevens voor dienen aan te leveren.

Weer vertraging

Het gevolg van het verschoningsverzoek nu is dat de behandeling van de beide zaken vertraging oploopt. Deze rechtszaken komen niet zo maar uit de lucht vallen en hebben een wat langere voorgeschiedenis. Op 13 november 2013 had de rechtbank Amsterdam al vernietigend geoordeeld over de goedkeuring die het CBP oorspronkelijk had gegeven aan de toentertijd door de zorgverzekeraars voorgestelde gedragscode omdat deze het medisch beroepsgeheim miskende en inbreuk maakt op de fundamentele bescherming van de privacy van patiënten. Dat komt omdat door de koppeling van de verwerking van medische persoonsgegevens aan uiteenlopende 'bedrijfsprocessen' als kwaliteitsbewaking, marketing en zorgbemiddeling geen sprake is van de door het EVRM vereiste helder en limitatief omschreven doelstelling van gegevensverwerking, en de toetsing op proportionaliteit en subsidiariteit niet kan doorstaan. De rechtbank had daarbij uitdrukkelijk gewezen op de taak van het CBP als toezichthouder om ervoor te zorgen dat zorgverzekeraars zich houden aan de wettelijke kaders van de Wbp en EVRM; heel specifiek aan de wijze waarop eerdere rechterlijke uitspraken (van het College voor Beroep en bedrijf) daarbij hadden bepaald dat patiënten en zorgverleners nimmer gedwongen mogen worden om voor declaratiedoeleinden aan de verzekeraars vertrouwelijke diagnose-informatie af te staan.(tekst in hyperlink van Vrijbit)

Daarna heeft de AP, als opvolger van het CBP, lang getreuzeld met reageren.

Hinderlijk

Ronduit hinderlijk was de wijze waarop de geplande zitting van de zaak UTR 16/3326 WBP V97 op 30 september 2016 uitgesteld

moest worden, omdat de AP na eerder door haar gevraagd uitstel niet tijdig de benodigde dossierstukken aanleverde. In een zo lang lopende zaak is het verre van professioneel als de vereiste stukken niet op tijd ingeleverd worden en riekt het naar obstructie.

Vraag

Het is raadselachtig waarom daags voor een zitting in een zo lang lopend juridisch gevecht in een principiële kwestie een rechter vraagt om niet opgesteld te worden. Het is de vraag of de betreffende rechter eigenstandig tot die beslissing gekomen is vanwege partijdigheid/nevenfunctie of dat de overige rechters hebben aangedrongen op het doen verschonen. Het trieste is dat het vragen van een rechterlijke uitspraak over het handelen of liever gezegd niet handelen van de AP zo een zeer moeizame zaak wordt.

In een democratische rechtsstaat moet het toch mogelijk zijn een toezichthouder ter verantwoording te roepen.

Want anders kan men zich alleen maar, met de dichter Juvenalis (ca. 60 – tussen 133 en 140 na Chr.), vertwijfeld afvragen: “Quis custodiet ipsos custodes”

(*Wie zal de bewakers zelf bewaken?)*

W.J. Jongejan

Psychiatrie-afdeling UMCU balanceert op randje met big-data-analyse

Op 16 juli stond in het Financieel Dagblad(FD) een uitgebreid artikel van redacteur Marieke ten Katen met als titel: "Gedwongen opname? Op dag vijf zal de patiënt agressief zijn". (1). Het gaat over de experimenten met big-data-analyse, die onder leiding van afdelingshoofd psychiatrie van het Universitair Medisch Centrum Utrecht(UMCU) Floor Scheepers(kinder – en jeugdpsychiater) sinds begin 2015 uitgevoerd worden met geanonimiseerde patiëntengegevens. Het betreft data uit 8000 patiëntendossiers. Het artikel vermeldt de steun van de Raad van Bestuur van het UMCU, met name van vicevoorzitter Frank Miedema. De initiatiefneemster is onder de indruk van de mogelijkheden van big-data-analyse en ziet mogelijkheden, voor de psychiatrie, maar ook voor chronische ziekten als kanker, ziekte van Parkinson en dementie om met big-data-analyse nieuwe wegen in te slaan. De doelstelling is om tot software te komen, die een risicoprofiel kan opstellen van een patiënt en ook een persoonlijke behandeling kan voorstellen. Het gaat dus om een vergaande vorm van "profiling". Profiling kent echter grote gevaren. Het belangrijkste gevaar is volgens Merel Eilander, woordvoerster bij de Autoriteit Persoonsgegevens, dat een patiënt anders wordt behandeld op grond van iets wat je zelf niet bepaald hebt of kunt controleren. Daarmee komt de individuele vrijheid in het geding. Software die drijft op de input van big-data

zou een hulpmiddel moeten zijn, maar wordt in de praktijk vaak een alziend oog dat als vrijwel onfeilbaar beschouwd wordt. Teruggaand naar de titel van het artikel in het FD kan op basis van big-data-analyse daar eigenlijk alleen staan ”Gedwongen opname? Op dag vijf **kan** de patiënt in vergelijking met andere dagen agressief zijn”. De huidige titel straalt iets absoluuts uit.

Beperkingen

Binnen het UMCU realiseert men zich terdege dat er grote privacy-problemen ontstaan als de eigen geanonimiseerde database gekoppeld wordt aan andere databases met persoonsgegevens, zoals die van het Centraal Bureau voor de Statistiek(CBS). Koppeling van een database met geanonimiseerde of gepseudonimiseerde gegevens aan een andere met dezelfde voorzorgen kan bij voldoende dataoverlap en sophisticated software altijd leiden tot de mogelijkheid gegevens tot op een individu te herleiden. Daarom werd dat soort koppelingen tot nu toe in het UMCU nog niet tot stand gebracht. Er wordt nu geanalyseerd met geanonimiseerde data op groepsniveau, **nog niet** op het niveau van individuele patiënten. Koppelingen voerde men uit met open databronnen, zoals gegevens over het weer(KNMI) of data over de buurt waar een patiënt woont. Daarbij kan je bij de eerste bron je nog wel voorstellen dat het uitvoerbaar is om met volledig geanonimiseerde data te werken. In het voorbeeld van de buurtdata moeten minimaal de vier cijfers van de postcode uitgesloten zijn geweest bij de anonimisering, omdat anders een koppeling met buurtdata onmogelijk zou zijn geweest.

Blijkbaar verloopt het onderzoek dat men nu doet met de koppeling aan open data-bronnen zonder toestemming van de patiënt. De initiatiefneemster stelt namelijk dat als er koppelingen zouden gaan plaatsvinden met bijvoorbeeld bepaalde CBS-gegevens toestemming van de patiënten nodig is, vanwege het herleidbaar worden van gegevens op individueel niveau. Dat

is ook het officiële standpunt van de Autoriteit Persoonsgegevens(AP). Naar mijn idee dient echter elk onderzoek dat gebruikt maakt van patiëntgegevens aanleiding te zijn voor een gesprek met de patiënt, waarin men diens toestemming vraagt om de gegevens te verwerken.

Lastig

Het UMCU is in gesprek met juristen en patiënten en gaat **vooralsnog** niet over tot koppelingen aan andere databases met persoonsgegevens. Het wordt bij lezing van het artikel tussen de regels door wel als lastig ervaren. Dat woord neemt ook de jurist Maarten Goudsmit, werkzaam bij het grote advocatenkantoor Kennedy van der Laan halverwege het artikel in de mond. Deze verwijst ook naar uitspraak van de AP, waarin deze stelt dat medische gegevens moeilijk te anonimiseren zijn en dus toestemming aan de betrokken patiënten gevraagd moet worden. Bij een big-data-project vindt Goudsmit dat vragen om toestemming ronduit lastig. Hij schaart zich met dat standpunt automatisch bij de pro big-data lobby. De ondertoon bij dit deel van het artikel is duidelijk. De Wet bescherming persoonsgegevens en de uitleg die de AP daaraan terecht geeft staat naar het oordeel van voorstanders van big-data-analyse ongelimiteerd gebruik van zorggegevens in de weg. In een eerder artikel legde ik uit dat aan de vereisten in het kader van de Wet bescherming persoonsgegevens, namelijk doelbinding, proportionaliteit en subsidiariteit bij big-data-analyse van zorggegevens eigenlijk nooit voldaan kan worden. Dat betekent ook weer niet dat daarom die wet daarom afgeschaft of veranderd moet worden.

Commercie

Dat de commercie zeer duidelijk geïnteresseerd is in deze schoorvoetende opening richting big-data-analyse blijkt wel uit de onbetaalde steun die volgens het artikel het UMCU kreeg van onder andere het data-adviesbureau GoDataDriven, dat meerdere hackathons organiseerde. Daarbij kijken

datawetenschappers zonder medische achtergrond met grote inzet in een beperkte tijd(dag of weekend) naar data om te zien of er onvermoede verbanden te leggen zijn. GoDataDriven is zeker geen filantropische instelling. Op haar website wordt gewag gemaakt van projecten die liepen bij grote bedrijven als Bol.com, Wehkamp en Schiphol. Men zal alleen maar onbetaalde steun leveren als in de nabije toekomst toch commerciële opdrachten van het UMCU te verwachten zijn.

Oprekken

Het siert uitgerekend een afdeling psychiatrie van een universitair medisch centrum, die zeer privacygevoelige informatie onder haar beheer heeft, niet dat ze zelf het initiatief neemt voor enige vorm van big-data-analyse. Woorden als “nog niet” en “vooralsnog” wijzen op het willen doorzetten van de nu gepubliceerde intentie. In de wetenschap dat men direct dan wel indirect meewerkt aan het oprekken of ter discussie stellen van bestaande wet- en regelgeving over de bescherming van persoonsgegevens had een terughoudender opstelling van de afdeling psychiatrie en de raad van bestuur, van meer wijsheid getoond. Per saldo legt men op deze wijze het vertrouwen van de patiënt, die de meest intieme zaken aan de arts c.q. de psychiater toevertrouwt, in de waagschaal. Men balanceert zo op de rand van de afgrond.

W.J. Jongejan

(1) Het artikel uit het Financieel Dagblad zit achter een betaalmuur, maar met een gratis registratie kunt u 5 artikelen per maand van het Financieel Dagblad gratis online inzien.

Autoriteit Persoonsgegevens ondergraaft stelselmatig eigen gezag

Het is opvallend hoe de Autoriteit Persoonsgegevens(AP), voorheen het College Bescherming Persoonsgegevens(CBP) al enige tijd opereert bij geconstateerde overtredingen. Ondanks het feit, dat die hebben plaatsgevonden is steevast het beleid om bij het beloven van beterschap geen sancties op te leggen. Volstaan wordt met de waarschuwing, dat het na beloofde verbeteringen niet weer mag gebeuren. Deze halfslachtige houding voedt de gedachte, dat de AP een toezichthouder is die de bij wet verkregen tanden(per 1 januari 2016 nog aangescherpt) niet wil laten zien door geen sancties op te leggen. Daardoor ontstaat het beeld, dat de AP een verlengstuk is van de wetgever en uitsluitend de implementatie van wetten met zachte hand corrigeert en helpt uitvoeren. Ze wordt het verlengstuk van de politiek en geen krachtige, onafhankelijke, toezichthouder. Het speelt eigenlijk bij alle zaken die de AP onderzoekt, maar twee onderzoeken die van groot belang zijn voor de privacy van de burger, licht ik er voor u uit.

Suwinet

Dit is een besloten systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen in het kader van werk en inkomen. Een onderdeel van het UWV (Uitvoerings-instituut

WerknemersVerzekeringen) ondersteunt, beheert en ontwikkelt het verder. Via diverse applicaties bestaat toegang tot (persoons)gegevens van burgers, waaronder financiële data. De bronhouders van de gegevens zijn onder andere de Gemeentelijke Sociale Diensten, het UWV en de Sociale VerzekeringsBank, maar ook de belastingdienst en de rijksdienst voor het wegverkeer. Naast deze partijen hebben ook de Immigratie- en NaturalisatieDienst, de Inspectie SZW, gemeentelijke belastingdeurwaarders, gemeenten in het kader van de meld- en coördinatiepunten voortijdig schoolverlaters en de Stichting Netwerk Gerechtsdeurwaarders toegang tot het netwerk. Er zijn veel protocollen en richtlijnen voor de toegang gemaakt, maar daar bleek een meerderheid van de gemeenten zich niet aan te houden. Mensen die geen toegang zouden moeten hebben tot het systeem kregen dat wel, ook personeel van externe bureaus, die door gemeenten ingehuurd waren. Ook werd het Suwinet in enkele gevallen gebruikt voor een ambtelijk doel waarvoor het niet opgezet was, namelijk het parkeerbeheer. Veel overtredingen constateerde de AP bij onderzoek. Op 21 januari 2016 verscheen dat rapport over overtredingen bij 11 van de 13 onderzochte gemeenten. Wat gebeurt er? De AP maant de overtreders, volgt ze door een vervolgonderzoek te doen, maar legt geen enkele sanctie op aan de overtreders, die geacht werden te weten hoe het wel zou moeten.

DIS

De afgelopen jaar heeft de AP zich ook beziggehouden met de rechtmatigheid van het doorleveren van gegevens uit het DBC-Informatie Systeem(DIS) door de Nederlandse Zorgautoriteit(NZa) aan derden. Nadat eerst de organisatie DBC-onderhoud de verantwoordelijkheid droeg voor het DIS werd op 1 mei 2015 die verantwoordelijkheid ondergebracht bij de NZa. Het ging om ge-pseudonimiseerde zorggegevens, die bij nadere beschouwing toch herleidbaar waren tot individuen. De AP was tot dat onderzoek min of meer gedwongen door publiciteit omtrent de herleidbaarheid. De AP was al eerder op

de hoogte van deze materie o.a. door de uitzending van de tv-rubriek Zembla in 2014. Het komt uiteindelijk tot een uitspraak van de AP over dit onderwerp op 7 maart 2016. Daarin zegt de AP dat de gegevensverzameling van het DIS op zich wel rechtmatig is, maar dat doorlevering aan derden, zoals bijvoorbeeld de minister van VWS en het Centraal PlanBureau niet rechtmatig is. Het conceptrapport legde de AP eerst aan de NZa voor en paste het na een reactie van de NZa alsnog aan. Hoor en wederhoor bij mogelijke overtredingen hoort er te zijn, maar dat hoort plaats te hebben voor enig rapport uitgebracht wordt. Het voorleggen van een concept-rapport aan een onderzochte instantie is in mijn ogen al een zwaktebod. En wat gebeurt er met de geconstateerde overtredingen. De NZa belooft het niet meer te doen. De AP heeft daar vervolgens vrede mee ZONDER sancties op te leggen vanwege de begane overtredingen.

Vergelijking

De handelswijze van de AP ten aanzien van geconstateerde overtredingen is heel vreemd. Het is hetzelfde als wanneer een dief betrapt is op een serie diefstallen, belooft het niet meer te doen en vervolgens geen straf krijgt opgelegd.. De handelswijze van de AP strookt absoluut niet met het rechtsgevoel, omdat organisaties waar de AP toezicht op houdt zo altijd wegkomen bij overtredingen zonder sancties. Het is bijvoorbeeld bij de Autoriteit Financiële Markten(AFM) niet voor te stellen, dat een overtreder met de belofte het nooit meer te doen geen sanctie opgelegd krijgt.

Uiteindelijk ondergraaft deze uiterst zwakke handelswijze van de AP het vertrouwen van de burgers in de overheid. Een sterke en ferm optredende toezichthouder is in het belang van burger en overheid.

Zachte heelmeesters maken nu eenmaal stinkende wonden.

W. J. Jongejan

Opt-in-vraag LSP door thuiszorg strijdig met Wbp

Recent schreef ik op deze website een artikel over het gaan vragen door thuiszorgmedewerkers van de opt-in-toestemming voor elektronische gegevensuitwisseling via het Landelijk SchakelPunt(LSP). Hierin gaf ik aan dat het vragen van deze toestemming, door een ander dan de brondossierhouder onfatsoenlijk, ongewenst en illegaal is. In Nijmegen is een taskforce om het aantal opt-in-toestemmingen te maximaliseren aan de slag gegaan met het idee de thuiszorg daarbij in te schakelen. Bij bestudering van wat in de Wet bescherming persoonsgegevens(Wbp) staat en de uitleg die de Autoriteit Persoonsgegevens(AP) daarbij geeft is duidelijk dat als de opt-in-toestemming verkregen wordt bij een ander dan de brondossierhouder er sprake is van overtreding van artikel 33 en 34 van de Wbp. Van deze overtreding is door mij melding gemaakt bij de Autoriteit Persoonsgegevens. Op 18 juli berichtte de AP dat de brief daarover in goede orde ontvangen was.

Wetsartikelen

Hoofdstuk vijf van de Wbp gaat over de informatieverstrekking aan de betrokkene(patiënt) en de meldplicht bij inbreuken op de beveiliging van persoonsgegevens aan het College. Met

College wordt het College Bescherming Persoonsgegevens(CBP) bedoeld, de rechtsvoorganger van de Autoriteit Persoonsgegevens(AP). In de artikelen 33 en 34 wordt duidelijk omschreven dat de verantwoordelijke(de brondossierhouder in dit geval, dus de huisarts of apotheker) vóór de verwerking van de gegevens de betrokkene(de patiënt) voorlicht om die geggevens daarna(met toestemming van de patiënt) te verwerken. Artikel 34 lid 4 kan bij de LSP-opt-in niet van toepassing zijn. Daar staat een uitzondering voor het geval het verkrijgen van de toestemming een onevenredige moeite zou kosten. Dat is niet het geval want voor het Nijmeegse initiatief was er in die regio al een redelijk toestemmingspercentage.

De tekst van de artikelen luidt:

Artikel 33

1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Artikel 34

1. Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede,

bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is: **a.** op het moment van vastlegging van hem betreffende gegevens, of **b.** wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
4. Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.
5. Het eerste lid is evenmin van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

Uitleg AP

Op de website van de Autoriteit Persoonsgegevens kan men ook een duidelijke uitleg vinden van wat in artikel 33 en 34 Wbp staat. Deze uitleg sluit ook uit dat een ander dan de brondossierhouder een opt-in-toestemming voor elektronische gegevensuitwisseling via het LSP vraagt. Het is alleen bij de AP de vraag of deze door de politiek bewust onderbemande dienst met een veel te laag budget het handhaven in deze kwestie ook ter hand neemt.

Thuiszorg

Hoewel de thuiszorgorganisaties in 2015 reeds in de koepeladviesraad van de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ), als beheerder van het LSP, zijn opgenomen, is er geen sprake van het bijhouden van een aan het LSP gekoppeld brondossier bij die organisaties. Bij veldproeven in de regio Dordrecht/Gorinchem bleek dat het werken met het LSP in pilot-verband niet goed verliep. Daarbij kon bij de thuiszorgorganisatie de daar verantwoordelijke arts ouderenzorg alleen maar een medicatieoverzicht opvragen zonder eigen data via het LSP aan te kunnen leveren. Datgene wat geprobeerd werd lukte slecht en stuitte op grote mandateringsproblemen, waardoor men er mee stopte. Het opgenomen zijn in de koepeladviesraad van VZVZ zegt dan ook totaal niets over het gekoppeld zijn van thuiszorgsystemen aan het LSP.

De aanwezigheid in de koepeladviesraad kan dus nooit een legitimatie zijn voor hetgeen de taskforce in Nijmegen nu uitvoert. Ik ben zeer benieuwd of de AP hier actief gaat handhaven. De AP is het wel aan zijn stand verplicht dit te doen.

W.J. Jongejan

Vreemde deal Google met NHS-ziekenhuizen. Nederland geen haar beter

Recent kwam via een publicatie op de website van de New Scientist naar buiten dat Google via een bedrijf, DeepMind, dat men in 2014 opkocht voor 400 miljoen Pound Sterling, toegang krijgt tot zorggegevens van enkele miljoenen mensen. Die data zijn afkomstig uit drie ziekenhuizen van de Royal Free Trust in Londen. Ze vallen onder de National Health service(NHS). Het gaat om de gegevens van de ongeveer 1,6 miljoen mensen die jaarlijks die ziekenhuizen bezoeken. Ook wordt toegang verkregen tot de door die ziekenhuizen opgeslagen zorggegevens van de afgelopen vijf jaar. Aanvankelijk leek het erop dat de deal tussen Google en de Royal Free Trust alleen over acuut nierlijden zou gaan, maar de nu bekend geworden samenwerkingsovereenkomst laat zien dat het om een veel meer data van legio ziekten gaat. De overeenkomst met een commerciële partij die aan data-mining doet roept veel vragen op. Zowel wat privacy betreft als ook over de wenselijkheid een dergelijk bedrijf te faciliteren bij het exploreren en exploiteren van medische gegevens. In Nederland is het geen haar beter. Tot voor zeer kort konden gegevens uit het DBC InformatieSysteem(DIS) door derden gebruikt worden voor nadere analyse.

DeepMind

Dit bedrijf is een Britse start-up die zich bezighoudt met kunstmatige intelligentie en die gebruikt om medische expert-programma's/apps te ontwikkelen. De bedoeling is om bijv. te kunnen voorspellen welke patiënten grotere kans op

complicaties hebben. In februari van dit jaar leek het erop dat DeepMind met de genoemde NHS-ziekenhuizen alleen een deal had gesloten om een app, Streams, te kunnen maken die acute nierbeschadiging snel kan opsporen. Naar nu blijkt behelst de overeenkomst de verwerking van veel meer gegevens van de in de ziekenhuizen behandelde patiënten. Het gaat om de naar schatting 1,6 miljoen mensen die in 2016 de ziekenhuizen zullen passeren. Daarenboven krijgt DeepMind toegang tot de gegevens van alle patiënten die de laatste vijf jaar de ziekenhuizen bezochten. In de overeenkomst staat op pagina 3 waarvoor de data gebruikt worden.

"Outputs include tools toe enhance adherence to, and implementation, of, NHS/NICE guidelines. This will consist of: (i) Patient Safety Alerts for Acute Kidney Injury, and (ii) Real time clinical analytiscs, detection, diagnosis en decision support to support treatment and avert clinical deterioration across a range of diagnoses and organ systems."

Het gaat dus om veel meer dan alleen acute nierbeschadiging.

Beveiliging

Heel veel staat er in de overeenkomst over hoe de beveiliging van de data en de verwerking ervan geregeld is. De gegevens worden naar een Trusted Third Party gestuurd. Patiëntgegevens worden gepseudonimiseerd. Het vervelende van pseudonimisering is echter dat als er bij een big-data-analyse maar genoeg databestanden gekoppeld worden het zeer wel mogelijk is de identiteit van iemand te herleiden. Hoe meer data des te minder anoniem dus.

Privacy

Er wordt in het hele document met geen woord gerept over de toestemming van de patiënt om mee te werken. De NHS kent alleen een opt-out-principe. Van alle patiënten worden de gegevens gebruikt behalve van degenen die dat niet willen. Voor het komende jaar kunnen mensen eventueel nog aangeven

niet te willen dat hun gegevens gebruikt worden, maar voor de data die tot vijf jaar terug gebruikt mogen worden is dat niet mogelijk. Het opt-out-principe is een niet wenselijke toestemmingsvorm. In Nederland kennen we het opt-in-principe, waarbij verwerking in principe niet mag tenzij de patiënt toestemt. Bovendien zit de patiënt bij bezoek aan deze ziekenhuizen in een afhankelijkheidsrelatie waardoor weigeren psychologisch gezien moeilijk is.

Commercieel

De vraag is of je het laten analyseren van medische gegevens wel moet uitbesteden aan een zeer grote commerciële partij als Google. Google is geen filantropische instelling en staat bekend om haar verdienmodel op basis van data-mining. Door het samenwerken met een bedrijf dat wereldwijd opereert en met DeepMind een nieuw marktdeel verkent, werkt men mee aan een monopolie-positie van dat bedrijf op het vlak van het exploreren en exploiteren van medische data. In het bekend geworden samenwerkingsprotocol is nergens een financiële paragraaf te vinden. Ik kan me niet goed voorstellen dat de tegenprestatie van Google alleen de aangekondigde expertsoftware wordt die op basis van de data ontwikkeld gaat worden.

Nederland

Je zou denken, dat een dergelijke beschikbaarstelling van medische gegevens in Nederland niet voorkomt. Niets is minder waar. Wij kennen hier een heel grote database waarin van de diagnosegegevens van alle Nederlanders opgeslagen zijn. Het gaat om het DIS. Dat is het DBC Informatie systeem dat onder verantwoordelijkheid van de Nederlandse Zorgautoritei(Nza) opereert. Tot voor zeer kort(tot december 2015) konden derden bij de NZa een aanvraag indienen om de gepseudonimiseerde gegevens te mogen gebruiken voor analyses. Het was al langer duidelijk dat de gepseudonimiseerde DIS-gegevens te herleiden waren tot individuen. Vanaf 2008 heeft de Koepel van DBC-vrije

Praktijken(KDVP) al gezegd dat het DIS niet privacy-proof is. In 2015 gaf de NZa in een rechtszaak die de Open State Foundation had aangespannen, toe dat de DIS-gegevens tot personen herleidbaar waren. Daarop besloot de NZa eind 2015 de gegevens vooralsnog niet aan derden te verstrekken. Het College Bescherming Persoonsgegevens(CBP), nu Autoriteit Persoonsgegevens(AP) hield lange tijd vol dat het niet ging om persoonsgegevens, en stond doorlevering aan derden toe. Nadat de NZa had toegegeven dat de data niet echt anoniem zijn, besloot de AP een onderzoek in te stellen, want als het om bijzondere, want medische, persoonsgegevens handelt kan doorlevering aan derden niet plaatsvinden. In januari 2016 kwam de AP met een oordeel. Zorgverleners dienen de gegevens alleen nog maar anoniem, d.w.z. zonder de (direct en indirect) identificerende kenmerken aan te leveren. Bovendien moet er een andere oplossing komen voor de pseudonimisering van de gegevens. Gedacht wordt aan het tussen schakelen van een Trusted Third Party. Aan welke derden men gegevens uit het DIS verstrekt, wordt eigenlijk nergens duidelijk. Hoewel Google wel niet bij het DIS zal hebben aangeklopt, is het zeer wel mogelijk dat in Nederland medische data ten onrechte door derden zijn geanalyseerd.

Resourcegrabbing

Wat we met de deal van Google zien is eigenlijk een vorm van resource-grabbing. Grote spelers op de wereldmarkt pogen lucratieve deelmarkten te exploreren en verkregen informatie dan wel ervaring te gebruiken in hun businessmodel. De jurist Ab van Eldijk, voorzitter van de KDVP schreef er een zeer lezenswaardig artikel over. Google zet dan eens hier, dan eens daar, veel geld in om nieuwe deelmarkten te verkennen, maar stoot daarbij weleens de neus. In 2014 nam het voor 500 miljoen dollar Boston Robotics over, een bedrijf dat veelbelovend leek met zich zelf voortbewegende, soms humanoïde robots. Dit jaar zette Google het bedrijf weer in de verkoop en verschoof de aandacht naar het analyseren van medische

data. Het al te makkelijk denken van zorginstellingen of koepelorganisaties over het beschikbaar stellen van die data faciliteert bedrijven die medische data willen gebruiken voor hun eigen verdienmodel.

W.J. Jongejan

07-05-2016 08.40u: Niet werkende link naar artikel Ab van Eldijk hersteld.

Verbieden Whatsapp bij artsen klein bier voor in grote privacy-zaken stille Autoriteit Persoonsgegevens

Al enige tijd, maar vooral na de jaarwisseling, laat de Autoriteit Persoonsgegevens(AP), voorheen het College bescherming Persoonsgegevens(CBP), van zich horen door het doen van ferme uitspraken. Het gaat dan bijna altijd om privacy-gaan, die op de keper beschouwd als “klein bier” te beschouwen zijn. Zo ging het in januari 2016 ook over camera’s in sauna’s. en in vrachtwagencabines. Grote privacy-zaken

worden mondjesmaat aangepakt. Privacy-zaken die de samenleving op dit moment sterk bezig houden, zoals de schendingen van privacy in de jeugdzorg en rond de Suwinet-problematiek krijgen nauwelijks aandacht. Doorzettingsmacht toont de AP daarin nauwelijks. Vaak wordt eerder aangestuurd op nieuwe wetgeving om privacy-gaten te dichten dan dat de AP er uitspraken over doet.

Whatsapp

De aanleiding voor het schrijven van dit artikel is de ruime aandacht in de media die het verbieden van het gebruik van WhatApp door artsen kreeg. De AP meldt op de website van Medisch Contact zelfs dat een individuele arts een bestuurlijke boete opgelegd kan krijgen als de privacy van een patiënt geschonden is. Krachtige taal, maar uit de AP zich altijd op diezelfde wijze bij andere zaken? Laat de AP de tanden wel echt zien bij grote schendingen van de privacy? Helaas moet aan de hand van enkele voorbeelden vastgesteld worden dat die fermheid toch heel beperkt is en vrijwel nooit getoond wordt als het gaat door privacy-overtredingen door de lokale of hogere overheden.

Undermanned/Understaffed

De privacy-waakhond is door de politiek met financiële middelen fors gemuilkorfd. In het afscheidsinterview in de NRC van de voormalige voorzitter van het CBP, Jacob Kohnstamm, gaf hij aan dat een vervijfvoudiging van het budget nodig was om het CBP, Nu AP, naar behoren de taken te laten verrichten. Er kwam geen budgetverruiming, waardoor de AP zelf aangeeft per jaar maar 15 tot 20 grote zaken te doen. Het is daarbij ook maar de vraag wat onder groot verstaan wordt.

Jeugdzorg-1

Bij de grote veranderingen in de zorg speelt ook de overheveling van de jeugdzorg richting gemeenten wat betreft het uitvoeren en de financiering. Inmiddels is het wijd en

zijd bekend dat binnen de gemeenten teveel mensen, meestal zonder medische beroepsgeheim weet hebben van de meest gevoelige details van cliënten. Gegevens worden gecommuniceerd over onbeveiligde verbindingen. Het meest stuitende is dat de ouders van cliënten onder druk worden gezet bij de huisarts het volledige medische dossier uitgeprint op te vragen en te overhandigen aan niet aan enig beroepsgeheim gebonden gemeenteambtenaren. Bij bezwaren krijgt men te horen dat er anders niet over de casus beslist kan worden. Horen we hier de AP krachtig over oordelen en gemeenten openlijk dreigen met boetes? Neen.

Jeugdwet-2

Op dit moment is er een veegwet voor de jeugdzorg in de maak, wetsontwerp 34111. In de eerder van kracht geworden Jeugdwet staat in artikel 7.4 dat de Colleges van burgemeester en wethouders van gemeenten verplicht zijn om incidenteel dan wel systematisch informatie verkregen in het kader van de jeugdhulpverlening door te leveren aan de ministers van Volksgezondheid, Welzijn en Sport en aan die van Veiligheid en Justitie. Het is bedoeld voor het gebruik bij beleidsontwikkeling, maar kan onvoorzien toch een eigen leven gaan lijden. Over dat soort onderwerpen spreekt de AP bij het maken van de genoemde veegwet af en toe mee, maar er wordt naar buiten toe geen duidelijk signaal over afgegeven. Daardoor is alles niet bepaald transparant.

Suwinet

Dit is de koppeling van diverse grote overheidsbronbestanden waardoor veel data van een burger in één klap opgevraagd kunnen worden. Het is opgezet in het kader van de wet Syri, afkorting van Systeem Risico Indicatie. Jacob Kohnstamm noemde het als voorzitter van het CBP zelfs een regelrechte ramp. Recent bleek dat van een steekproef bij dertien gemeenten slechts bij twee de protocollen en hantering op orde waren. De AP schetste bij het publiceren van het onderzoek toch nog een

rooskleurig beeld. Er viel niets te bespeuren van bestuurlijke dwang, geen dreigement met boetes. Eerst gaat men de betrokken gemeenten weer wat maanden volgen en daarna beslist men weer verder.

LSP

Ook bij het Landelijk SchakelPunt(LSP) is er niet sprake van spraakmakende acties. Bij de start werd een beoordeling van het doorstartmodel gegeven dat positief was, maar het toenmalige CBP stelde toen zelfs al dat zulks niets zei over het daadwerkelijke functioneren. Een beoordeling van de praktijk daarvan heeft tot heden niet plaatsgevonden. Een onderzoek over het geven van opt-in-toestemmingen leverde een flink aantal manco’s op. Het CBP koos niet voor het gelijk publiceren van die manco’s en krachtige taal uitslaan, maar liet de beheerder van het LSP, VZVZ eerst weerwoord EN correctie van gemaakt fouten toe, alvorens een gematigd oordeel publiek te maken.

Brede borst

De Autoriteit Persoonsgegevens wekt de indruk vooral een ferme indruk te wekken in kleinere privacy-zaken die niet direct overheden betreffen. Waar het overheden betreft is er dan geen ferme standpuntbepaling, maar vaak een sturende beweging naar een in de ogen van de AP redelijke oplossing. Daarbij wordt ook nog weleens een signaal richting politiek afgegeven om het gemelde probleem door weer nieuwe wetgeving op te lossen.

W.J. Jongejan

Autoriteit Persoonsgegevens schetst te rooskleurig beeld veilig gebruik Suwinet

Op 21 januari 2016 publiceerde de Autoriteit Persoonsgegevens(AP), voorheen het College Bescherming Persoonsgegevens(CBP), een overzicht over hoe het gesteld is met de navolging door gemeenten van de richtlijnen voor het gebruik van Suwinet. De AP stelt bij monde van haar vice-voorzitter Wilbert Tomesen dat de situatie verbeterd is en dat een aantal gemeenten voldoet aan de norm, maar ook dat er nog steeds gemeenten zijn die dat niveau niet bereikt hebben. Hij wijst wel op de gevaren van het niet goed op orde hebben van de zaken vanwege de mogelijke inbreuken op de privacy. Toch blijft bij lezing van de stukken de indruk hangen dat alles nog veel te rooskleurig wordt voorgesteld..

Suwinet

Suwinet is een besloten systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen in het kader van werk en inkomen. Via Suwinet kan veel informatie over iemand worden verkregen. Dit kan bijvoorbeeld gaan om gegevens over arbeidsverleden, opleiding, alimentatie, uitkering of boetes. (Woorden AP). Door de koppeling van een aantal grote bron-gegevenshouders is het van eminent belang dat de toegang tot de gekoppelde systemen goed geregeld, uitgevoerd en gehandhaafd wordt. Op zich is Suwinet al door de schaalgrootte een discutabel systeem vanwege de implicaties voor de privacy. Als ook de

toegang niet goed geregeld blijkt te zijn en de handhaving van de regels dan bestaat er een nog groter maatschappelijk probleem.

Omvang

Waar de AP spreekt over het onderzoek bij de gemeenten gaat het slechts om een steekproef van slechts 13, variërend van klein tot groot, van alle Nederlandse gemeenten. De AP, onderbemand als ze al tijden is, zou ook geen grotere steekproef aankunnen. Van deze 13 gemeenten waren er slechts twee die alle zaken administratief volledig op orde hadden. Het waren niet geheel toevallig beide grote gemeenten die ongetwijfeld een eigen IT-afdeling en eigen IT-management in huis hebben. Dat is iets wat bij de kleinere gemeenten vaak stiefmoederlijk bedeeld is.

Veel mis

In het overzicht van de conclusies van het onderzoek bij de dertiengemeenten blijkt vooral dat het gaat om het niet hebben van een goedgekeurd beveiligingsplan en het niet goed controleren van de toegangsrechten tot Suwinet, Daarbij is dan ook sprake van het ontbreken van een correcte autorisatie. Het zijn allemaal overtredingen van artikel 13 van de Wet bescherming persoonsgegevens(Wbp). In één gemeente, Nunspeet, was sprake van een medewerker die toegang had tot Suwinet ten behoeve van de naleving van de Algemenen Plaatselijke Verordening(APV), parkeerbeheer en het bevolkingsonderzoek. Er is volgens de AP totaal geen wettelijke grondslag voor raadpleging van persoonsgegevens voor het toezicht op die zaken. Daardoor is er sprake van het overtreden van artikel 8 van de Wbg. Wat hier duidelijk wordt hoe makkelijk er sprake is van illegale “function-creep”. Vanwege de beschikbaarheid van een zoeksysteem wordt er gewoon gebruik van gemaakt, ook al is het doel van dit systeem anders. Het is schokkend te constateren dat lagere overheden in deze steekproef vrij massaal de wet overtreden.

Tucht

Bij dit alles moet men bedenken dat zonder de controles van de AP de onderhavige gegevens niet boven water zouden zijn gekomen. Na bekendmaking van de resultaten van het onderzoek aan de gemeenten en voor algemene publicatie mochten de gemeenten nog een zienswijze inleveren om te beargumenteren dat de AP mogelijk stukken niet goed begrepen had en extra materiaal aan te dragen. Daarnaast maakten meerdere gemeenten in de zienswijze kenbaar dat ze de boodschap van de AP begrepen hadden en hun procedures inmiddels aangepast hadden. Het onderzoek had duidelijk een corrigerend effect.

Triest

Gezien de omvang van de steekproef en het totale aantal gemeenten in Nederland(390 per 01-01-2016) is het dus duidelijk slecht gesteld met de navolging van het beschikbare normenkader voor het gebruik van Suwinet door de gemeenten. Gemeenten blijken in groten getale regelgeving betreffende privacy-gevoelige informatie niet op te volgen of de gebruiksgrenzen op te rekken. In wezen is er bij het gebruik van Suwinet sprake van een privacy-gevoeligheid die in de buurt komt van de medische datacommunicatie. Daar is de autorisatie en authenticatie geregeld door UZI-passen, kaartlezers en pin-codes terwijl bij de gemeenten sprake is van een blijkbaar slecht gestructureerde toegang tot Suwinet.
Het verhaal dat de Autoriteit Persoonsgegevens thans brengt, laat de negatieve punten wel zien. Er is een duidelijke PR-saus over gegoten door de nadruk te leggen op het verbeteren van de situatie en het voldoen van enkele gemeenten aan de normen. Het wordt eigenlijk gebracht als een soort nul-meting die voor verbetering vatbaar is. Helaas gaat het dan wel om slechts twee van de onderzochte dertien gemeenten en is het Suwinet al enige tijd in gebruik.
Het vertrouwen in hen die over ons gesteld zijn neemt door dit alles niet toe, terwijl de lokale overheid wel het goede voorbeeld zou moeten geven bij het navolgen van de wetgeving van de centrale overheid.

W.J. Jongejan.

Onderbezetting toezichthouder privacy(CBP) is politieke keuze

Op de webpagina van het NRC-Handelsblad staan op 30 december 2015 een tweetal artikelen die gebaseerd zijn op een openhartig interview met Jacob Kohnstamm, voorzitter van het College Bescherming Persoonsgegevens(CBP). Het eerste heeft als kop "Privacy kan mensen wél wat schelen", het tweede de kop: "Privacywaakhond CBP kampt met onderbezetting" (overigens ook deels op www.nu.nl te lezen). Kohnstamm geeft er in aan dat privacy wel degelijk een belangrijk item is. Hij noemt persoonsgegevens ook het nieuwe goud. Daarnaast geeft hij een zeer sterk signaal af dat het CBP zwaar onderbezet is. Hij zegt duidelijk dat er minstens vijf keer zoveel personeel als er nu bij het CBP is, een goed begin zou zijn omdat anders de handhaving van de privacywetgeving in het gedrang komt. Hij heeft meerdere keren bij de politiek neergelegd dat er meer geld en mensen nodig zijn voor de huidige taken plus de uitbreiding door het ingaan van nieuwe regelgeving, maar kreeg nul op het rekest.

Autoriteit Persoonsgegevens

Jacob Kohnstamm werd geïnterviewd vanwege de naamsverandering van het CBP per 1 januari 2016. Het College Bescherming Persoonsgegevens gaat dan Autoriteit Persoonsgegevens heten. Het lijkt een naam die gezag moet uitstralen, maar de mogelijkheden om dat te doen zijn beperkt door de onderbezetting. Het CBP ontstond in 2000 uit de Registratiekamer en staat te boek als een zelfstandig bestuursorgaan gerelateerd aan het ministerie van Veiligheid en Justitie. Overigens zal Kohnstamm per 1 augustus 2016 het voorzitterschap neerleggen.

Onderbezetting

Eigenlijk is het CBP al vanaf het ontstaan een organisatie geweest die "undermanned and understaffed" is. Men heeft continu keuzes moeten maken wat wel of niet aangepakt moest gaan worden. Ook in het beoordelen van sommige zaken heeft het ook geschort aan voldoende en goede oordeelsvorming. Zo moest bijv. in 2013 het CBP een draai van 180 graden maken ten aanzien van haar eerdere goedkeringsbesluit betreffende de Gedragscode Zorgverzekeraars. Ook het stelselmatig ontwijkend reageren op het verzoek tot handhavend optreden tegen de onrechtmatige verwerking van gegevens in het DIS(DBC-Informatie-Systeem), als één van de grootste en meest risicovolle databanken van Nederland, is er een uiting van. Hier ligt een rechterlijke uitspraak van het College van Beroep voor het bedrijfsleven aan ten grondslag. Ook gaf het CBP in januari 2012 ten aanzien van het Landelijk SchakelPunt(LSP) slechts een beoordeling van het doorstartmodel van de Vereniging voor Zorgaanbieders Voor Zorgcommunicatie(VZVZ) vanuit de situatie dat de minister van VWS er verantwoordelijk voor was. Van de toen aangekondigde beoordeling van de daadwerkelijk gegevensuitwisseling in de praktijk is nooit iets terecht gekomen. In 2014 kwam het CBP ook met een halfzachte beoordeling van het verkrijgen van de opt-in-toestemmingen voor het LSP. Met een zeer beperkte

steekproef, waren er best wel flinke missers. Het CBP rapporteerde echter pas, nadat VZVZ in staat was gesteld eerst een aantal missers te corrigeren.

Het nieuwe goud

Vanaf 1 januari 2016 treedt de meldplicht datalekken in werking en mag het CBP als kersverse autoriteit Persoonsgegevens hoge boetes opleggen in plaats van voorwaardelijke dwangsommen. Op 1 januari 2017 komt er de implementatie van Europese privacyregels bij. Het CBP werkt nu met 80 mensen, waarvan er 60 daadwerkelijk toezicht uitoefenen op de privacy. Desondanks moet Kohnstamm na verzoeken om uitbreiding van formatieplaatsen constateren dat er geen budget voor uitbreiding komt. Volgens Kohnstamm heeft het ministerie wel beloofd het budget van zijn organisatie opnieuw te overwegen als blijkt dat er zeer veel datalekken worden gemeld. Met de huidige bezetting kan het CBP maar 15 tot 20 grote zaken per jaar aan. De ambitie van Kohnstamm is echter meer en hij maakt zich dan ook terecht bezorgd over bedrijven die met “big data” verzameld via allerhande apps en websites aan “profiling” van de klant doen. Hij noemt “big data” ook het nieuwe goud. Het zoeken naar big data door grote bedrijven is te beschouwen als het fenomeen van “resource grabbing” en heeft dringend regelgeving nodig, zeker nu medische data ook onderdeel van “big data” zijn.

Kort houden

De enige conclusie die er getrokken kan worden bij het lezen van de woorden van Jacob Kohnstamm en bij een nauwkeurige beoordeling van wat het CBP vermag, is dat de overheid, c.q. de minister van Veiligheid en Justitie het CBP heel duidelijk kort houdt. Daardoor is het CBP niet in staat adequaat zaken aan te pakken. Kohnstamm stelt terecht dat privacy voor de burger wél wat kan schelen. De overheid laat merken door de zeer beperkte financiering dat privacy bij haar geen hoge prioriteit heeft. Het is weer een voorbeeld dat papier alles

klopt maar dat de werkelijkheid net iets anders ligt.

Eigenlijk heeft wat er nu gebeurt met het CBP duidelijke parallellen met de gang van zaken rond de Nederlandse Voedsel en Waren Autoriteit. Die is ook bewust te klein gemaakt en valt onder een ministerie waar het economische belang van de agrariërs zwaarder telt dan de voedselveiligheid.

Het signaal dat Kohnstamm nu afgeeft moet beschouwd worden als een urgente “wake-up-call”, een beroep op de overheid om op een fatsoenlijke manier recht te doen aan de privacy van de burgers, die zij vertegenwoordigt. Helaas zijn de signalen die de overheid afgeeft over de privacy van burgers niet hoopgevend.

W.J. Jongejan