21-11-2016 Nadere notitie Burgerrechtenvereniging Vrijbit bij zaaknummer UTR 16/4199 WBP V93.

Bij de start van het DIS (DBC InformatieSysteem) heeft het CBP(nu AP) nadrukkelijk gesteld (zie bijlage 1: brief CBP van 10 januari 2006) “dat het DIS zowel qua omvang, dekking als inhoud een van de meest risicovolle verwerkingen binnen Nederland zal zijn”. Deze constatering van de toezichthouder had betrekking op een informatiesysteem dat nadrukkelijk geacht werd geen tot personen herleidbare gegevens te verwerken.

Het DBC Informatie Systeem DIS zoals dat in 2006 is gestart bestaat uit een database waaraan procedures zijn gekoppeld voor verplichte aanlevering van medische gegevens zonder dat de patient daar toestemming voor heeft gegeven en omvat tevens procedures voor de doorlevering van deze medische gegevens. Doorlevering van medische gegevens vond ondermeer plaats via reguliere, vaste koppelingsprocedures met een groot aantal publieke partijen als ook enkele private partijen zoals CvZ, DBC-onderhoud. Tevens konden medische gegevens uit het DIS op aanvraag worden doorgeleverd aan andere partijen (zie bijlage 2: meer in het bijzonder hoofdstuk 2 van dit visiedocument over de verwerking van behandelgegevens).
Zoals aangegeven in de documenten die zijn ingebracht bij de aan dit beroep voorafgaande bezwaarprocedure, moet de toezichthouder gedurende lange tijd hebben geweten dan wel geacht worden te hebben geweten dat de geanonimiseerde dan wel gepseudonimiseerde medische gegevens zoals die ontvangen, verwerkt, doorgeleverd en gebruikt worden door het DIS, herleidbaar zijn tot personen. Bijgevolg is het DIS (de database met de daaraan gekoppelde procedures) komen te vallen onder de werking van het bepaalde in Wbp en EVRM.

In de brief van 10 december 2006 stelt de toezichthouder hierover zeer nadrukkelijk het volgende:

> “ Zodra niet (meer) aan de bovengenoemde voorwaarden wordt voldaan, is sprake van persoonsgegevens en zijn WBP en medisch beroepsgeheim 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 in DIS geen rechtsgrond bestaat, zou in dat geval sprake zijn van een onrechtmatige gegevensverwerking*. Het blijven voldoen aan de gestelde voorwaarden vereist dus continue inspanning.
>
> 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. Dit soort gegevens heten 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 levensscyclus van het DIS bij wijziging van de gegevenssets en overigens periodiek te worden herhaald”.*

Deze stellingname doet duidelijk uitkomen dat het doen aanleveren, verwerken, doorleveren en gebruiken van indirect herleidbare medische gegevens via dit “qua omvang dekking en inhoud meest risicovolle informatiesysteem in Nederland” onrechtmatig is omdat daarvoor geen rechtsgrond bestaat.

Dat de toezichthouder niet onmiddellijk heeft ingegrepen door handhavend op te treden nadat de herleidbaarheid van gespeudonimiseerde medische gegevens (van alle Nederlanders!) onomstotelijk was aangetoond, is niet alleen verwijtbaar onzorgvuldig, maar had de toezichthouder er ook toe moeten brengen om na te gaan welke partijen betrokken zijn geweest bij betreffende onrechtmatige verwerking van medische persoonsgegevens teneinde verder gebruik en doorlevering van deze gegevens te voorkomen door betrokkenen te wijzen op het onrechtmatige karakter van deze gegevensverwerking.

Gezien hierboven aangehaalde stellingname van de toezichthouder is het onbegrijpelijk en onjuist dat de toezichthouder niet alleen heeft afgezien van ingrijpen, maar zelfs de logging van uitgeleverde/doorgeleverde gegevens niet heeft opgevraagd teneinde zicht zo zicht te krijgen op aard en omvang van het gebruik van medische persoonsgegeven die onrechtmatig zijn verkregen via het DIS. Onderzoek naar doorlevering en gebruik van onrechtmatig verwerkte medische gegevens had direct dienen plaats te vinden toen de toezichthouder kennis kreeg van de herleidbaarheid van bij het DIS aangeleverde medische gegevens. Waar dit ten onrechte is nagelaten had handhavend optreden tenminste gestart moeten worden in reactie in reactie op het ingediende handhavingsverzoek.

Door tijdig op te treden tegen de verwerking van medische persoonsgegevens bij het ontbreken van de noodzakelijke wettelijke grondslag kon en kan voorkomen worden dat onrechtmatig verkregen medische persoonsgegevens op grote schaal gebruikt werden door tal van publieke en private partijen die deze gegevens via het DIS hebben verkregen.

Het is onjuist dat de AP nu meent alle leveranties aan publieke en private partijen buiten beschouwing te kunnen laten waar deze niet op de wet maar op enige afspraak/overeenkomst zijn gebaseerd. Dit is onjuist omdat daarmee ten onrechte niet wordt opgetreden tegen het gebruik, het verdere gebruik en mogelijke doorlevering van onrechtmatig verkregen medische persoonsgegevens.

De conclusie van de AP dat doorgifte, verwerking en gebruik van medische persoonsgegevens door tal van publieke en private partijen buiten beschouwing kan worden gelaten nu het verstrekken van deze gegevens is stopgezet “vanaf het moment dat de Autoriteit Persoonsgegevens heeft aangegeven zich te beraden op haar standpunt ten aanzien van het karakter van de DIS-gegevens”, gaat voorbij aan de verantwoordelijkheid van betrokken partijen voor gebruik, verder gebruik en doorlevering van onrechtmatig verkregen medische persoonsgegevens.

Gelet op het feit dat het hier gaat om een van de grootste datalekken (zie bijlage 3 Platform bescherming burgerrechten: Autoriteit Persoonsgegevens moet optreden tegen het grootste datalek van Nederland) vanuit één van de meest risicovolle data systemen van Nederland, had de toezichthouder, gelet op het grote maatschappelijke belang (zie ook bijlage 4: Alex Brenninkmeijer, Geloofwaardig toezicht) verbonden met deze grootschalige verwerking van medische persoonsgegevens, handhavend/corrigerend moeten optreden tegen betreffende onrechtmatige gegevensverwerking om de gevolgen daarvan te beperken. Dit handhavend optreden had ook gericht moeten zijn op de zorg TTP die tot taak had er op toe te zien dat medische gegevens verkregen via het DIS niet konden worden herleid tot personen. Gelet op het ontbreken van de noodzakelijke wettelijke grondslag (wet informele zin) voor het verwerken van medische persoonsgegevens had de zorg TTP verantwoordelijk moeten blijven voor de verwerking van medische persoonsgegevens via het DIS.

Waar de toezichthouder concludeert dat de levering van medische persoonsgegevens aan NZa , ACM, CBS en Zinl legitiem is voorzover de verstrekking van deze gegevens plaats vindt op grond van een wettelijke bepaling, wordt ten onrechte voorbij gegaan aan de verplichting om - op grond van Wbp en EVRM – de noodzaak tot het verwerken van medische persoonsgegevens voor een welbepaald doel afdoende te motiveren door deze verstrekkingen te toetsen aan kernwaarden van Wbp en EVRM. De toezichthouder heeft hier eerder zelf op gewezen (zie bijlage 5: CBP advies van 6 juni 2007, kenmerk z2006-01238) door te stellen dat:

> " Wel moet ……worden onderbouwd waarom bepaalde persoonsgegevens noodzakelijk zijn bij de uitvoering van een bepaling, noodzakelijk om een bepaald doel te bereiken……. Om te kunnen beoordelen of de noodzaak daadwerkelijk bestaat, waarbij de beginselen van proportionaliteit en subsidiariteit een rol spelen, is een expliciete onderbouwing van de noodzaak – eventueel per onderdeel van een artikel – noodzakelijk".

Er ontbreekt echter een afdoende onderbouwing, motivering van bepalingen in de Wmg en in de "Regeling categorieën persoonsgegevens Wmg" voor een doelgebonden doorlevering en verwerking van medische persoonsgegevens door onderscheiden publieke en private partijen (NZa, ACM, ZiNL, CBP, FIOD-ECD en CBS). Dit is des te opmerkelijker aangezien het toenmalige CBP (nu AP) bij de oprichting van het DIS had vastgesteld dat - met uitzondering van het CBS, die overigens ook gehouden is aan internationale verdragen incl. EVRM - verwerking van medische persoonsgegevens niet noodzakelijk was voor de onderscheiden instanties die gegevens vanuit het DIS aangeleverd kregen.
Gelet op de uitgebreide, zeer specifieke en zeer gevoelige persoonsgegevens die middels de aan te leveren *"Minimale" Data-Set* (zie bijlage 6) - zonder toestemming van de patiënt met doorbreking van het medisch beroepsgeheim - moeten worden aangeleverd bij het DIS is het begrijpelijk dat aanlevering van dit soort informatie op de persoonsniveau niet geacht wordt noodzakelijk/proportioneel te zijn voor beleidsinformatie.

Waar het bij het verkrijgen van beleidsinformatie gaat om toetsing aan het subsidiariteitsbeginsel verwijzen we graag naar de conclusies in onderdeel 4.6 van het visie document de verwerking van behandelgegevens opgenomen in bijlage 2.

Met betrekking tot de verplichting tot aanlevering van medische persoonsgegevens (zonder toestemming van de patiënt en met doorbreking van het medisch beroepsgeheim) aan de NZa is het bepaalde in artikel 61 Wmg nog steeds te algemeen geformuleerd en niet welbepaald om te kunnen spreken van een legitieme, noodzakelijke aanlevering van medische persoonsgegevens. Volgens de bewoordingen van de Wmg is het aan de NZa als vrager om te bepalen welke gegevens moeten worden verstrekt omdat deze door haar *redelijkerwijs van belang kunnen worden geacht* (zie ook oordeel over deze formulering bij punt 3.5 in CBP-advies opgenomen in bijlage 5) voor de uitvoering van taken. Dit kan worden getypeerd als een formulering van een discretionaire bevoegdheid en zeker niet als een formulering die past bij een gemotiveerde, noodzakelijke verstrekking van medische persoonsgegevens door zorgverleners met doorbreking van het medisch beroepsgeheim.

Het enkele feit dat DBC-onderhoud (gestart als private organisatie met als enig doel - zonder eigen belang bij de verwerking van informatie - het ontvangen en verwerken van medische gegevens door het DIS) is ondergebracht bij de NZa maakt gebruik en doorlevering van medische persoonsgegevens door de NZa op zich niet legitiem. Daarvoor is, zoals hiervoor opgemerkt, een getoetste en gemotiveerde wettelijke bepaling nodig waarmee de noodzaak van de inbreukmakende verwerking kan worden gelegitimeerd. De in de Wmg geformuleerde (discretionaire) “bevoegdheid” om medische persoonsgegevens te verwerken voor zover dit *naar het oordeel van de NZa noodzakelijk is* wordt in artikel 2 van de “Regeling categorieën persoonsgegevens Wmg” nadrukkelijk ook van toepassing verklaard op medische persoonsgegevens.
We moeten echter vaststellen dat noch het onderbrengen van DBC-onderhoud bij de Nza, noch de nadere regelgeving in de “Regeling categorieën persoonsgegevens Wmg” de specifieke grondslag kan vormen voor de verwerking van bijzondere persoonsgegevens door de NZa. Wil de gezochte aanlevering (met doorbreking van het medisch beroepsgeheim), verwerking, doorlevering en gebruik van medische persoonsgegevens via het DIS legitiem zijn dan moet dit gebaseerd zijn op een bepaling in een wet in formele zin, voorzien van een dragende motivering die verwijst naar de toetsing aan kernwaarden van Wbp en EVRM.

Het voorstel tot aanpassing van de Wmg (33980) dat nu bij de Eerste Kamer ter beoordeling voorligt moet, nadat het CBP jaren geleden al had gewezen op de noodzaak om de Wmg aan te passen wegens het ontbreken van een specifieke wettelijke grondslag (in wet in formele zin)voor de verwerking van bijzondere persoonsgegevens in overeenstemming met vereisten vastgelegd in Wbp en EVRM (zie bijlage 7: CBP advies van 13 april 2005, kenmerk: z2005-0070 en het CBP advies van 6 juni 2007, kenmerk: z2006-01238 opgenomen als bijlage 5, alsook bijlage 8: uitspraak Rechtbank Gelderland 16-8-2016 en bijlage 9 blz. 111,112 en 113 van RUG publicatie 2016, Rechtsstatelijke aspecten van de decentralisaties in het sociale domein) Het standpunt van het CBP bij de start van het DIS over aanlevering, verwerking, doorlevering en gebruik van medische gegevens via het DIS, maakt duidelijk dat de toezichthouder de verwerking van medische gegevens op

persoonsniveau niet noodzakelijk achtte voor de verschillende beleidsondersteunende doelstellingen waarvoor het DIS werd opgericht.(zie in bijlage 2: hoofdstuk 2 van visiedocument over de verwerking van behandelgegevens)

De voornaamste bezwaren die tegen deze aanpassing van de Wmg (33980) worden ingebracht hebben betrekking op het opheffen van het medisch beroepsgeheim, het opheffen van vertrouwelijkheid bij medische zorgverlening zonder dat sprake is van een noodzakelijke inbreuk op de privacy van patiënten en het medisch beroepsgeheim die toetsing aan de beginselen van proportionaliteit, subsidiariteit en voorzienbaarheid kan doorstaan.

Door NZa en AP wordt ten onrechte voorbij gegaan aan de geconstateerde ernstige gebreken van de Wmg met als gevolg de grootschalige en onrechtmatige verwerking van medische persoonsgegevens door tal van publieke en private partijen die medische persoonsgegevens hebben verkregen via het DIS-informatiesysteem.

Op grond van voornoemde feiten en overwegingen zijn we dan ook van mening dat de AP als toezichthouder vanaf 2005 regelmatig is geconfronteerd met regelingen (aanpassing van publieke wet- en regelgeving), procedures (o.a. m.b.t. doorlevering op basis van afspraken/contracten) en verwerkingspraktijken (herleidbaarheid) die wegens het ontbreken van de noodzakelijke wettelijke grondslag resulteerden in onrechtmatige verwerking en gebruik van medische persoonsgegevens.
Dat ondanks het grote publieke belang niet handhavend is opgetreden tegen het onrechtmatig verwerken en gebruiken van medische persoonsgegevens moet op zich reeds worden aangemerkt als verwijtbaar onzorgvuldige handelen van de toezichthouder en moet er naar ons oordeel toe leiden dat de toezichthouder ingevolge deze beroepsprocedure - gericht tegen het afwijzen van handhavend op treden bij de onrechtmatige verwerking van medische persoonsgegevens via het DIS door de verschillende betrokken partijen - alsnog wordt verplicht handhavend op te treden tegen alle patijen betrokken bij aanlevering, verwerking, doorlevering en gebruik van onrechtmatig verkregen medische persoonsgegevens.

Voor zover aanpassing van de Wmg zoals geformuleerd in wetsvoorstel (33980) wordt betrokken bij de oordeelsvorming in deze procedure, willen we er nogmaals op wijzen dat ook deze toekomstige wetgeving toetsing aan kernwaarden van Wbp en EVRM op geen enkele wijze kan doorstaan.