Uitspraak Autoriteit Persoonsgegevens gaat ook andere be-/verwerkers zorgdata aan

Op 16 december 2019 deed de Autoriteit Persoonsgegevens(AP) uitspraak over het gepseudonimiseerd verzamelen van zorgdata. Het betrof de Routine Outcome Monitoring(ROM)-gegevens uit de geestelijke gezondheidszorg(GGZ). De Stichting Benchmark GGZ(SBG) verzamelde die en overhandigde die bij bedrijfsbeëindiging aan de opvolger Akwa GGZ De uitspraak van de AP was vernietigend. De vraag is of de uitspraak van de AP geen consequenties heeft voor allerhande dataverzamelingen in de zorg waarbij sprake is van be-/verwerking van gepseudonimiseerde zorgdata. De AP stelde vast(pag.19 punt 4.2.3 in link) dat SBG op hun gepseudonimiseerde dataset onvoldoende technische waarborgen en/of maatregelen had genomen om de risico's op herleidbaarheid, koppelbaarheid en deduceerbaarheid in voldoende mate weg te nemen. Om zo te kunnen spreken van een anonieme dataset. Het risico op indirecte herleidbaarheid was in onvoldoende mate weggenomen. Het is de vraag of andere bedrijven en instellingen die zich met zorgdata-verzamelen bezig houden ook niet fout bezig zijn.

Gepseudonimiseerde data verzamelen

Met zorgdata legt men op diverse plaatsen gigantische dataverzamelingen aan om daarop allerlei be-/verwerkingen uit te voeren. Een voorbeeld van een dergelijke dataverzamelingen is het DBC Informatie Systeem(DIS) waarin alle Diagnose-Behandel-Combinaties(DBC) van alle Nederlanders die in een ziekenhuis behandeld worden staan. Het DIS be-/verwerkt ook

gepseudonimiseerde data. De wijze van pseudonimiseren is onbekend. Een andere grote dataverzamelaar is het Dutch Institute for Clinical Auditing(DICA). Daarnaast bestaan vele anderen. DICA doet naar eigen zeggen het volgende. *"DICA verricht klinische registraties en levert daarmee betrouwbare analyses en vergelijkingen aan de zorgverleners en eventuele andere partijen. Met de verzamelde gegevens kan DICA clinical audits uitvoeren die tot doel hebben om onderzoek/metingen naar kwaliteit van zorg te doen."* DICA maakt daarbij gebruik van het bedrijf Medical Research Data Management(MRDM) als IT-partner en gegevensbewerker van het ziekenhuis, in het kader van DICA-registraties. MRDM bewerkt de patiëntgegevens zodanig dat DICA alleen gecodeerde (pseudoniem) gegevens ontvangt.

Hoe gepseudonimiseerd?

Het rapport n.a.v. het onderzoek naar gegevensverwerking door SBG van de AP gaat vrij ver in op de technische wijze waarop SBG de pseudonimisering liet verrichten. De AP stelt bijv. dat er geen gebruik wordt gemaakt van enige vorm van randomisatietechnieken op het moment dat SBG de dataset ontvangt. Men stelt vast dat t. a.v. het zogenaamde generaliseren de techniek van aggregeren (niet k-anonimiteit) wel gezien is, maar niet toegepast. De eindconclusie was dat door risico's als herleidbaarheid, koppelbaarheid en deduceerbaarheid niet met het door SBG gebruikte anonimiseringsproces weggenomen werd. Daardoor was de herleidbaarheid tot de persoon nog steeds mogelijk doordat de persoon geïdentificeerd wordt door een unieke waarde na pseudonimisering. Aangezien dezelfde unieke (gepseudonimiseerde) waarden door de tijd samengevoegd dienen te worden is risico op koppelbaarheid even groot. Tot zover de technische details. Het is volmaakt onduidelijk of alle rond de zorg actieve data-verzamelaars en be-/verwerkers wel voldoen aan de eis van afdoende blokkering van de herleidbaarheid van een individu.

Uitzonderingsgronden

De bedrijven die de data be-/verwerken zullen veelal aan te merken zijn als verwerkingsverantwoordelijke in de zin van artikel 4, onderdeel 7 van de Algemene Verordening Gegevensbescherming(AVG). Als er niet sprake is van een afdoende vorm van pseudonimisering dan is er sprake van de verwerking van bijzondere persoonsgegevens . Het is dan de vraag of de bedrijven die grootschalig data verwerken net als SBG zich niet kunnen beroepen op één van de algemene uitzonderingen zoals opgenomen in artikel 9, tweede lid, onderdeel j van de AVG (juncto artikel 24 UAVG) op het verwerkingsverbod van bijzondere categorieën. De data verwerkende bedrijven zijn namelijk geen instelling voor gezondheidszorg of maatschappelijke dienstverlening.

Wat gaat de AP doen?

De vraag is wat de AP na deze uitspraak gaat doen. Laat men het erbij en hoopt men dat de uitspraak een zelfregelend effect gaat hebben op bedrijven in de zorg die gepseudonimiseerde data be-/verwerken? Of spreekt de AP die sector nu actief aan teneinde de huidige uitspraak meer kracht te kunnen bijzetten. En controleert ze. Het zou best eens kunnen zijn dat SBG als bedrijf het topje is van een ijsberg waarvan het grootste deel nog buiten zicht is.

Medische data worden tegenwoordig als het nieuwe goud gezien. Bedrijven als Google en Apple storten zich erop. Het dus van groot belang dat medische data in wat voor soort database dan ook goed beschermd zijn en bij be-/verwerking er niet sprake kan zijn van enige directe of indirecte herleidbaarheid tot een individu.

De zaak rond SBG en Akwa GGZ dient een les te zijn. Waarbij we dan wel moeten bedenken dat het boven water komen ervan het gevolg is van de vasthoudendheid van één persoon.

W.J. Jongejan, 20 december 2019

Afbeelding van Okan Caliskan via Pixabay