Je kon er op wachten: groot datalek zorggegevens gemeente Amersfoort

Terwijl in de huisartsenwereld inmiddels wijd en zijd inmiddels bekend is dat persoons-/zorggegevens van patiënten niet per gewone e-mail verstuurd moeten worden, blijkt men bij gemeenten er een andere moraal op na te houden. Bij de gemeente Amersfoort verstuurde een ambtenaar meerdere weken geleden gegevens van 1900 burgers, afkomstig van de sociale wijkteams per mail naar een verkeerde persoon. De gegevens betreffen naam, adres, burgerservicenummers, maar gaan ook om de omschrijving van geleverde (jeugd)zorg. Op diverse websites zoals van SKIPR, RTVUtrecht en het Algemeen Dagblad wordt er melding van gemaakt. Nog kwalijker is dat men het voor de eigen wethouder en burgemeester geheim hield. Ook meldde men het niet aan de Autoriteit Persoonsgegevens. Op niet melden staat sinds 1 januari 2016 een boete van ruim achthonderdduizend euro. Uit de berichten blijkt dat de verantwoordelijke wethouder pas enkele dagen geleden is ingelicht. Het is te hopen dat die inmiddels aangifte heeft gedaan van dit datalek bij de Autoriteit Persoonsgegevens.

Zorgen

Al langere tijd hebben zorgkoepels als de KNMG en, LHV, maar ook organisaties die zich bezig houden met de privacy van burgers grote zorgen geuit over de uitvoering van de

(jeugd)zorg door de gemeenten. Zowel intern als naar extern schort het aan het bewaren en bewaken van het medisch beroepsgeheim. Veel deelnemers aan sociale wijkteams die niet onder het medisch beroepsgeheim vallen hebben inzage in zeer gevoelige persoonlijke, medische gegevens. Daarenboven vragen de wijkteams bij behandelende artsen veel meer gegevens op dan relevant voor de te geven en door de gemeenten te vergoeden zorg.

Twee grote fouten

Naast de foute adressering zijn naar het zich laat aanzien de gegevens met gewone e-mail verzonden. Er is dan geen sprake van beveiligde (zorg)mail zoals die in de huisartsen- en ziekenhuiswereld gebruikt wordt. Daarnaast heeft geen cryptografische versleuteling van het bestand plaats gevonden waardoor de gegevens direct in te zien zijn.

Lessen

Er vallen zeer veel lessen te leren uit deze casus, niet alleen door gemeenten, maar ook door regering en parlement. Bij het overhevelen van taken naar de gemeenten, met name ten aanzien van de jeugdzorg is beslist onvoldoende gekeken naar de geheimhoudingsaspecten rond zorggegevens. De (medische) privacy is niet afdoende geborgd door wetsartikelen. Het parlement heeft onvoldoende oog gehad voor deze aspecten. Men heeft het de gemeenten zelf maar laten uitzoeken. Dit zijn daar nu de kwalijke gevolgen van.

Het hele proces van de omgang met privacy gevoelige informatie van burgers door gemeenten zal op de schop moeten.

Zo niet: dan kan men wachten op het volgende incident.

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.