



Gemeente Brummen

Rekenkamercommissie Brummen

REKENKAMERBRIEF “Privacy in de 3 decentralisaties”

INLEIDING

Door de 3 decentralisaties verwerkt de gemeente vanaf 1 januari 2015 veel meer persoonlijke en privacygevoelige gegevens. Daarmee worden zorgen om privacy (weer) reëel. Verontrustende berichten over het schenden van privacy in tijdschriften (onder meer Binnenlands Bestuur) en inspectierapporten (over veilig gebruik van Suwinet) bracht de Rekenkamercommissie (RKC) Brummen op de gedachte om een vooronderzoek te starten naar de borging van privacy bij de gemeente Brummen.

Het vooronderzoek startte september 2015 en bestond uit literatuuronderzoek en een verkennend gesprek met de Auditcommissie van Brummen.

Nu er een raadsvoorstel voorligt om “Kadernotitie gegevensverwerking en privacy in de 3 decentralisaties 2016-2018 en de bij behorende documenten vast te stellen”, heeft de RKC besloten om haar verkenningen rondom privacy in de 3 decentralisaties vóór de raadsbehandeling van genoemd voorstel in een rekenkamerbrief met uw raad te delen.

SAMENGEVAT

De RKC waardeert de stap die het college zet met de “kadernotitie gegevensverwerking en privacy in de 3 decentralisaties”. In de kadernotitie formuleert het college beleid om de privacy van inwoners te waarborgen. Er is echter meer nodig om de privacy van burgers te (waar)borgen. Met deze rekenkamerbrief aan de gemeenteraad vraagt de RKC aandacht voor structurele aanpak van privacy, voor de positie (en het vertrouwen) van de burger en voor bewustwording en daadkracht in eigen huis.

TOELICHTING

De “kadernotitie gegevensverwerking en privacy in de 3 decentralisaties” geeft richtlijnen voor het zorgvuldig omgaan met persoonsgegevens in de 3 decentralisaties in de gemeente Brummen. Het is een (beleids)kader dat (citaat pag. 2 kadernotitie) *“richtinggevend is voor alle organisaties, professionals en ambtenaren die bij de uitvoering van gemeentelijke taken in het sociale domein actief betrokken zijn.”*

De RKC wil het volgende onder de aandacht van uw raad brengen.

1. Eenduidig beleid is een noodzakelijke maar geen voldoende voorwaarde om de privacy van de inwoners te borgen

Raad, wees u ervan bewust dat de kadernotitie een onderdeel is van een privacy-raamwerk. Om privacy goed te regelen moeten er maatregelen genomen worden op vijf gebieden, die met elkaar samenhangen: governance, beleid, werkprocessen en triage¹, bewustwording en training, en beheer en opslag (zie bijlage 1 toelichting).

¹ Met triage wordt bepaald wanneer beslissingen over gegevensuitwisseling worden genomen.

Aandachtspunten

- Hoe is het gesteld met privacy in de werkprocessen, het (privacy-bewust) gedrag van gemeentelijk personeel (en partnerorganisaties) en beheer en opslag van gegevens? Zijn de privacy afspraken geïmplementeerd in de organisatie (governance)? Kortom: In welke mate zijn deze aandachtsgebieden “privacy-proof”?
- Wanneer en hoe gaat het college de genoemde aandachtsgebieden “privacy-proof” maken? Wat zijn de prioriteiten van het college?
- Hoe gaat het college de raad informeren en verantwoording afleggen over de aandachtsgebieden van het privacy-raamwerk? Waarover wil de raad minimaal geïnformeerd worden?

2. Het belang van de burger

De gemeente heeft de plicht om zorgvuldig om te gaan met de persoonsgegevens van haar burgers. Daar moet de burger van op de hoogte zijn.

Aandachtspunt

- Hoe gaat het college burgers informeren over de borging van “hun” privacy? En over de positie en rechten van burgers, zoals het opvragen van de eigen gegevens en klachtenafhandeling?

3. Bewustwording en daadkracht in eigen huis

De gemeente is verantwoordelijk voor het veilig gebruiken van persoonsgegevens.

Dat Brummen (en met Brummen vele gemeenten) dit onvoldoende op orde heeft in het domein werk en inkomen, blijkt uit inspectierapporten van het ministerie van SZW over Suwinet (zie bijlage 2).

Recent besteedde de NPO in een televisie-uitzending van “de monitor” aandacht aan de onzorgvuldige en onprofessionele manier waarop een aantal gemeenten omgaan met medische gegevens van jeugdigen in de jeugdzorg.²

Burgers hebben recht op een gemeentelijke overheid die zorgvuldig omgaat met persoonsgegevens en zeker met medische gegevens van burgers. Bewustwording en daadkracht in de gemeentelijke organisatie wat betreft privacy en veilig gebruik van persoonsgegevens is essentieel.

Aandachtspunten

- Hebben het inspectierapport van SZW over veilig gebruik van Suwinet (2015) en de aangekondigde acties voor verbetering geleid tot acties van het college? Welke acties gaat het college in het komend jaar uitvoeren? Wanneer gaat het college een zelftest uitvoeren ten aanzien van veilig gebruik van gegevens in Suwinet? En hoe staat het met de implementatie van BIG (Baseline Informatiebeveiliging Gemeenten) in de organisatie?
- Zijn er personen in de organisatie aangewezen of benoemd (waaronder een wethouder) die informatieveiligheid in portefeuille hebben? Overweegt het college dit te doen?
- Heeft het college zicht op de manier waarop Team voor Elkaar omgaat met medische gegevens van met name cliënten in de jeugdzorg? Hoe wordt er met medische dossiers omgegaan? Zijn er extra voorschriften (ten opzichte van andere klantengroepen) voor cliënten in de jeugdzorg?

² Terug te zien op www.npo.nl/de-monitor van 22 november 2015.

TOT SLOT

Met deze rekenkamerbrief aan de raad sluit de RKC haar vooronderzoek rondom privacy in de 3 decentralisaties af. De RKC zal vooralsnog geen onderzoek in de gemeente Brummen starten over privacy en veilig gebruik van gegevens van burgers.

Met vriendelijke groet,

Rekenkamercommissie Brummen

Eric Giesbers

voorzitter

Bijlage 1: Privacy-raamwerk

Om gemeenten te helpen privacy goed te waarborgen, heeft VNG een privacy raamwerk ontwikkeld. Het raamwerk toont vijf gebieden, die met elkaar samenhangen: governance, beleid, werkprocessen en triage, bewustwording en training, en beheer en opslag. Die vijf gebieden zijn randvoorwaarden om privacy in het sociaal domein goed te regelen.

Beleid: Bepaal het kader rond de verwerking van persoonsgegevens en gegevensuitwisseling, zowel beleidsmatig als juridisch.

Governance: Implementeer de afspraken in de organisatie. Wat zijn de privacy-afspraken? Wat zijn de rollen en verantwoordelijkheden, wie voert de regie, wie controleert, hoe wordt verantwoording afgelegd?

Werkprocessen & triage: Organiseer het werk rondom het omgaan met persoonsgegevens.

Bewustwording en training: Ontwikkel bewustzijn rondom privacy, om situaties te herkennen waar privacyvraagstukken spelen. Training en communicatie zijn essentieel.

Beheer en opslag gegevens: Bepaal hoe gegevens in systemen worden opgeslagen en gedeeld. Wie heeft toegang? Hoe lang blijven gegevens bewaard? Wat wordt opgeslagen?



Voor een toelichting op het privacy-raamwerk: zie www.visd.nl/visd/gegevensuitwisseling-en-privacy

Bijlage 2: Bewustwording en daadkracht

Dat privacy bij gemeenten vóór de 3 decentralisaties onvoldoende geborgd was, blijkt uit twee inspectierapporten van SZW (2013 en 2015) over het gebruik van Suwinet.

Gebruik Suwinet niet veilig

Suwinet is het computersysteem dat gebruikt wordt door CWI, UWV en gemeenten bij het uitvoeren van hun taken op grond van de Wet SUWI (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen). Met een paar muisklikken kunnen ambtenaren allerlei persoonlijke gegevens van burgers inzien, zoals huisadres, bankrekening, loon, hypotheek, studieschuld.

In november 2013 stelde de Inspectie SZW vast dat het zeer slecht gesteld is met de manier waarop gemeenten Suwinet hebben beveiligd en hoe gemeenten omgaan met de gegevens die zij uit Suwinet halen. De Inspectie heeft dit gemeten aan de hand van (slechts) 7 normen van de in totaal 115 normen die opgenomen zijn in het Normenkader Suwinet. Het gaat om normen die sinds de start van Suwinet in 2002 gelden. Maar 4% van de gemeenten bleek aan de 7 getoetste normen te voldoen. VNG startte daarna een verbetertraject en in 2014 heeft de inspectie SZW het onderzoek naar veilig gebruik van Suwinet nogmaals herhaald. Voor het landelijke representatieve beeld werden 78 gemeenten (uit het totaal van 403 gemeenten) onderzocht. Toen bleek 17 % van alle gemeenten te voldoen aan alle 7 normen. De gemeente Brummen was een van de onderzochte gemeenten en bleek niet te voldoen aan de gestelde eisen.

De RKC heeft deze bevinding ingebracht in een overleg met de Auditcommissie van Brummen op 22 september 2015. Dit was voor wethouder Paauw aanleiding om onderstaande informatie per mail aan de griffier te verstrekken.

Suwinet en de gemeente Brummen

Over het Suwinet-rapport schrijft wethouder Paauw het volgende (Email volledig citaat).

“Over het rapport Suwinet kan ik het volgende melden.

Uit het definitieve verslag van de bevindingen veilig gebruik Suwinet 2014 blijkt dat de gemeente Brummen niet voldoet aan de gestelde eisen. Het rapport ziet uitsluitend toe op de toepassing van Suwinet op het gebied van de WWB. De gehele uitvoering van de WWB heeft de gemeente Brummen uitbesteed aan de gemeente Apeldoorn. Omdat tussen de gemeente Apeldoorn en de gemeente Brummen onduidelijkheid heeft bestaan over de verantwoordelijkheid voor de informatievoorziening en –verstrekking is vanuit de gemeente Brummen niet tijdig gereageerd op de uitgezette vragen vanuit de inspectie. Nu blijkt dat, ondanks dat de gehele uitvoering van de WWB is belegd bij de gemeente Apeldoorn, de verantwoordelijkheid en dus ook de verantwoording over gebruik en het verstrekken van informatie daarover, is gelegen bij de gemeente Brummen. Hierdoor zijn er geen gegevens vanuit Brummen naar het rijk verzonden en zijn de resultaten in de eindrapportage dan ook navenant.

Uit de zelfevaluatie die de gemeente Apeldoorn heeft uitgevoerd blijkt dat voldaan wordt aan alle eisen welke in dit onderzoek zijn gesteld. Dat betekent dat derhalve ook de gemeente Brummen aan deze eisen voldoet. Er is derhalve geen sprake van enig veiligheidsrisico zowel bij de gemeente Apeldoorn als bij de gemeente Brummen!

De gemeente Brummen is bezig om de BIG (Baseline Informatiebeveiliging Gemeenten) te implementeren in de organisatie. Dit project wordt in 2015 afgerond en dient jaarlijks te worden geëvalueerd. Suwinet maakt hier onderdeel van uit.

De resultaten van het eindrapport beschouwende komen wij als gemeente Brummen tot de conclusie dat een aantal actiepunten opgepakt en geïmplementeerd dienen te worden in de gemeente Brummen.

Wij gaan op korte termijn formeel een security officer binnen de organisatie aanstellen. Deze security officer zal verantwoordelijk worden voor de uit te voeren actiepunten waaronder:

- Invullen zelfevaluatie Suwi
- Verdere implementatie BIG
- Contact met security officer Apeldoorn om alsnog de gegevens aan de inspectie te kunnen zenden

De security officer beheert de beveiligingsprocedures en rapporteert hierover aan het management en het College van B&W.

Een werkgroep binnen de VNG heeft informatie bij ons opgevraagd. Bovenstaand bericht is naar tevredenheid gedeeld.”