Geacht college,

Dagelijks produceren en delen wij als inwoners van Oss meer en meer gegevens. Dit doen we zowel bewust als onbewust, vrijwillig als onvrijwillig. Digitale dataverzameling en IT-systemen zijn zo in ons dagelijks leven en het functioneren van de overheid ingebakken, dat het geen abstract concept meer is, maar een belangrijk fundament van de samenleving is geworden.

De beveiliging van onze gegevens zou dat ook moeten zijn. Dit wordt helaas maar al te vaak niet serieus genomen. Tot welke desastreuze gevolgen dit kan leiden bij gemeenten, laat o.a. de hack bij Hof van Twente in 2020 zien, waar een te gemakkelijk wachtwoord van een medewerker de belastingbetaler uiteindelijk 4,2 miljoen euro heeft gekost. [1]

De SP vindt dat de inwoners van Oss recht hebben op digitale veiligheid en privacy. Zij moeten er op kunnen vertrouwen dat de overheid niet meer gegevens van hen verzamelt dan strikt noodzakelijk is, en dat deze gegevens en de systemen die voor de verwerking gebruikt worden ten alle tijden onder de verantwoordelijkheid van de gemeente vallen.

Daarom stelt de SP de volgende vragen aan het college met betrekking tot de I-strategie en data strategie:

1. Is het college het met de SP eens dat bescherming van gegevens van de Osse inwoner de hoogste prioriteit verdient bij de omgang met hun gegevens?

2. Het college erkent de “groeiende invloed van Internet of Things” (Referentie: blz. 7 I-strategie). Erkent het college dat er aan het gebruik van “smart” apparaten veiligheids- en privacyrisico’s kleven, zoals het ongemerkt verzamelen en doorsturen van data naar derde partijen? [2]

3. Wat is de mening van het college over het gebruik en de risico’s van “smart” apparaten binnen de gemeente?

4. Welke “smart” apparaten beoogt de college concreet in de komende 3 jaar te gaan gebruiken, en met welk doel?

1 https://www.rtvoost.nl/nieuws/2144191/schade-na-hack-hof-van-twente-loopt-op-tot-4-2-miljoen-euro-gemeente-wil-bedrag-verhalen

2 https://pointer.kro-ncrv.nl/je-slimme-verlichting-deelt-je-leven-met-de-hele-wereld

5. Met het onvermijdelijke gebruik van (cloud)systemen van derde partijen (zoals Microsoft) raakt de gemeente een deel van de controle over gegevensverzameling en -verwerking kwijt.

5a. Hoe is het eigenaarschap van de data in deze cloud door de gemeente gedefinieerd?
5b. Wie is in de gemeente verantwoordelijk voor de beveiliging van deze gegevens?

6. Is het college ervan op de hoogte welke gegevens van inwoners met andere partijen gedeeld worden in de samenwerkingsverbanden zoals gemeenschappelijke regelingen (GR'en) waar de gemeente Oss deel van uitmaakt?

6a: Zo ja: wie is bij deze gegevens verantwoordelijk voor de beveiliging hiervan?
6b: Zo nee: is het college bereid dit uit te zoeken en een verantwoordelijke voor beveiliging aan te wijzen?

7. Hoe gaat de gemeente ervoor zorgen dat de GR'en volgens de Osse I- en data-strategie gaan werken?

8. De I-strategie stelt: "medewerkers krijgen een opleidingsprogramma over informatiebeveiliging met een verplicht basis niveau." (Blz. 9).

8a. Aan welke groepen medewerkers wordt deze opleiding aanboden?
8b. Hoe en hoe vaak wordt de inhoud van deze opleiding geactualiseerd?
8c. Hoe en hoe vaak wordt de inhoud van deze kennis bij medewerkers getoetst?
8d. Zijn er consequenties als een medewerker niet aan dit basisniveau voldoet?

9. Heeft de gemeente Oss een cybercrisisplan klaarliggen om catastrofes zoals bij Hof van Twente te voorkomen?

10. Hoe goed kan de gemeente Oss blijven functioneren in een noodgeval, zoals sterk verminderde beschikbaarheid van IT-systemen?

De SP kijkt met belangstelling uit naar de antwoorden op deze vragen.

Met vriendelijke groet,

Quinten Braakman