

Fractie Socialistische Partij
T.a.v. Quinten Braakman

E-mail gemeente@oss.nl
www.oss.nl

Postbus 5
5340 BA Oss

Wilt u bij uw reactie de
datum van deze brief en
ons kenmerk vermelden?

Datum	Ons kenmerk	Behandeld door	Doorkiesnummer
<i>Datum van collegevergadering</i>			
Onderwerp			Aantal bijlagen
Artikel 41 vragen van de fractie SP over digitale veiligheid en privacy			--

Geachte heer Braakman,

U hebt het college op 8 december 2022 artikel 41 vragen gesteld. Deze vragen gaan over digitale veiligheid en privacy. In deze brief beantwoorden wij uw vragen puntsgewijs. Deze antwoorden sluiten tevens aan op de vragen die zijn gesteld tijdens de rekeningcommissie naar aanleiding van de bevindingen door de accountant op IT gebied.

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?

De bescherming van de gegevens van onze inwoners heeft voor ons de hoogste prioriteit.

2. Het college erkent de "groeïende 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?

Behalve onze kantoorautomatisering maken we ook gebruik van Internet of Things (IoT). We zijn ons ervan bewust dat het gebruik van IoT extra uitdagingen met zich meebrengt op het gebied van informatiebeveiliging en privacy. Denk bijvoorbeeld aan de beveiliging van onze rioolgemalen, camerasystemen, verkeersbeheersing en liften.

De Autoriteit Persoonsgegevens besteedt als nationaal toezichthouder ook aandacht aan dit onderwerp. Met name in relatie tot het thema "smart cities". De AVG geldt onverkort bij dit onderwerp als daarbij persoonsgegevens worden verwerkt. Het is daarbij goed om op te

merken dat het niet gezegd is dat bij IoT / smart city-oplossingen per definitie persoonsgegevens worden verwerkt.

Ten aanzien van de bescherming van persoonsgegevens – als deze worden verwerkt – sluiten we met leveranciers en andere partijen die namens de gemeente persoonsgegevens verwerken (en indirect eventuele derde partijen) een verwerkersovereenkomst af waarin we afspraken maken over de rechtmatige verwerkingen van persoonsgegevens. Op deze manier zorgen we ervoor dat leveranciers op de juiste manier omgaan met de persoonsgegevens van onze inwoners. Als gemeente maken we hierbij primair gebruik van de standaard verwerkersovereenkomst van de VNG.

De Baseline Informatiebeveiliging Overheid (BIO), het verplichte overheidsbrede normenkader voor informatiebeveiliging, bevat in de basis aandachtspunten voor IoT-beveiliging. Daarom passen we de BIO niet alleen toe op onze kantoorautomatisering, maar ook op IoT. Omdat de beveiliging van IoT bij vrijwel alle gemeentes achterloopt op de beveiliging van kantoorautomatisering, zullen we in de toekomst hier meer aandacht aan geven. De Informatiebeveiligingsdienst (IBD) van de VNG biedt hiervoor handreikingen en adviseert om IoT-(beveiligings)beleid te ontwikkelen.

3. Wat is de mening van het college over het gebruik en de risico's van "smart" apparaten binnen de gemeente?

Net als bij reguliere kantoorautomatisering moeten we bij de inzet van slimme apparaten ook rekening houden met informatiebeveiliging en privacy. We bepalen van tevoren de risico's en treffen maatregelen om de risico's te verkleinen tot een acceptabel niveau. Indien persoonsgegevens hierbij worden verwerkt, dan geldt zoals hierboven vermeld de AVG onverkort.

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

Het is slechts bij benadering te zeggen welke 'smart' apparaten de gemeente de komende 3 jaar gaat inzetten. De ontwikkeling hiervan gaat namelijk zo snel dat we dat nu nog niet concreet kunnen maken.

Wat we wel aan kunnen geven is dat:

We in het buitengebied smart-openbare verlichting inzetten. Dit zijn de sensoren voor dynamische fietspadverlichting, conform vastgesteld beleid 2015:

- geen veiligheidsrisico's doordat lokale gateways met externe partij/server verbonden zijn voor technisch inregelen, storing en herstelondersteuning door leverancier
- geen privacy risico's doordat alleen aan/uit en dimmen geregistreerd wordt, voor/na detectie via bewegingsmelders (geen camera's).

We maken gebruik van slimme Verkeers Regel Installaties (VRI)

- standaard veiligheidsrisico's (zie punt 5 Verkeer.nu) door connectie met externe partij/server voor dagelijks beheer, voor technische ondersteuning, voor uitvaldetectie en toekomstig voor toepassen van iVRI.
- Geen of door gebruikersovereenkomsten afgedekte privacy risico's van alle detectie. Waarbij voor fietsersoversteek beveiliging naast standaard bewegingsdetectie ook fietsersdetectie camera's gebruikt worden. Enkel de bewegingsgegevens worden opgeslagen, geen camerabeelden opslag in de camera of automatisch aanwezig, ook geen WiFi verbinding met de camera mogelijk. Enkel een vaste verbinding naar de VRI automatisch voor groenverlenging op aankomende fietsersgroepen.

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.

1. Hoe is het eigenaarschap van de data in deze cloud door de gemeente gedefinieerd?

Hoewel data in juridische zin geen eigenaarschap kent, voelt Oss zich verantwoordelijk voor al haar data. Het maakt hierbij niet uit of de gegevens in de cloud staan of lokaal op onze eigen systemen worden beheerd. Daarom is het van groot belang dat Oss goede afspraken maakt met de (cloud)leverancier. Zo eisen we bijvoorbeeld een ISO 27001 certificering inclusief Verklaring van Toepasselijkheid (VvT) voor informatiebeveiliging en sluiten we verwerkersovereenkomsten voor de bescherming en rechtmatige verwerking van persoonsgegevens

2. Wie is in de gemeente verantwoordelijk voor de beveiliging van deze gegevens?

Het eigenaarschap wordt vastgesteld op basis van het proces waar de gegevens voor nodig zijn. De proceseigenaar, die tevens lijnmanager is, is niet alleen verantwoordelijk voor de kwaliteit van zijn gegevens, maar is ook verantwoordelijk voor het treffen van de juiste beveiligingsmaatregelen en het voldoen aan de privacywetgeving.

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?

a. Zo ja: wie is bij deze gegevens verantwoordelijk voor de beveiliging hiervan?

b. Zo nee: is het college bereid dit uit te zoeken en een verantwoordelijke voor beveiliging aan te wijzen?

Onze FG heeft in het jaarverslag over 2021 geconstateerd dat een volledig overzicht van partijen waarmee een (verwerkers)overeenkomst is gesloten ontbreekt. Enkele teams hebben wel een eigen overzicht. Om uitbesteding, samenwerking en uitwisseling van gegevens met externe partijen goed te borgen heeft de FG aanbevolen om overzicht te houden op deze partijen. De verantwoordelijkheid voor de informatiebeveiliging en privacy is mede afhankelijk van de concrete situatie. Dit is met name van belang bij taken die de gemeente Oss mandateert of delegeert.

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

Vanuit gezamenlijk belang voor de kwaliteit van onze basisregistraties wordt al op verschillende manieren afstemming gezocht en samengewerkt met bijvoorbeeld BSOB en ODBN. Vanuit de I-strategie en dan met name vanuit de Datastrategie wordt deze samenwerking de komende jaren verder geïntensiveerd. Dit is een onderdeel van het programma Data en deze processen worden vanuit daar ook gefaciliteerd.

De I-strategie is een dynamisch document en wordt de komende jaren thematisch geconcretiseerd. Dit doen we ook samen met de gemeenschappelijke regelingen en binnen de verschillende netwerken.

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

1. Aan welke groepen medewerkers wordt deze opleiding aangeboden?

Het gaan dit programma vanaf volgend jaar verplichten voor zowel nieuwe (via onboarding) als bestaande medewerkers. Omdat dit tijd en forse inzet vraagt van medewerkers wordt dit opleidingsplan eerst gedetailleerder uitgewerkt en voorgelegd aan het directieteam en college. Op dit moment worden medewerkers via nieuwsartikelen op ons intranet gewezen op informatiebeveiliging en privacy. Ook zijn er via ons online Leerplein modules beschikbaar voor bewustwording rondom deze twee onderwerpen.

2. Hoe en hoe vaak wordt de inhoud van deze opleiding geactualiseerd?

Het programma wordt nog in detail uitgewerkt en krijgt een terugkerend karakter.

3. Hoe en hoe vaak wordt de inhoud van deze kennis bij medewerkers getoetst?

Hierover zijn nog geen definitieve afspraken gemaakt. Dit is onderdeel van het uit te werken opleidingsplan.

4. Zijn er consequenties als een medewerker niet aan dit basisniveau voldoet?

Hierover worden nog passende afspraken gemaakt.

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

Eind 2021 hebben we aan de hand van een reële casus een cybercrisis geoefend met het bestuur, de directie en andere belangrijke stakeholders. Kort na deze oefening was er een wereldwijde cyberdreiging (Log4Shell) waar ook Oss last van had. Hierdoor hebben we in korte tijd een cybercrisisorganisatie neergezet. Vervolgens zijn we in 2022 aan de slag gegaan met het maken van een cybercrisisplan. Dit plan biedt handelingsperspectief bij een cybercrisis voor met name het management, de directie en het bestuur.

Dit plan is niet openbaar in verband met gevoelige informatie die het bevat.

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

Vorig jaar zijn we gestart met het inrichten van bedrijfscontinuïteitsmanagement (BCM). Bij calamiteiten moet op basis van BCM de continuïteit worden gewaarborgd van onze meest kritische bedrijfsprocessen. Business Continuïteit is er op gericht de dienstverlening ongehinderd doorgang te laten vinden bij grote calamiteiten.

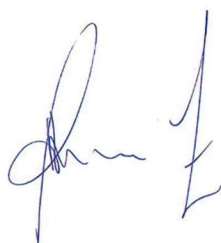
Er zijn per kritisch proces maatregelen in beeld gebracht en voor een groot deel ook al toegepast. In Q1 van 2023 wordt dit proces verder geborgd in de organisatie.

Met vriendelijke groet,

Burgemeester en wethouders van Oss.

De secretaris,

De burgemeester,



Drs. H. Mensink

Drs. W.J.L. Buijs-Glaudemans