

Onderwerp

Vragen m.b.t. de Kadernota BSOB 2026

Datum	24 februari 2025		
Afdeling	Financiën	Portefeuillehouder	Frank den Brok

Geachte leden van de gemeenteraad,

Tijdens de adviescommissie Sociaal Bestuurlijk van 6 februari 2025 zijn vragen gesteld m.b.t. het digitaliseringsbeleid van de BSOB. Ik heb de toezegging gedaan om schriftelijk te antwoorden. Hieronder volgt mijn beantwoording.

Vraag 1.

BSOB ambieert mutatiedetectie i.c.m. kunstmatige intelligentie en geautomatiseerd doorvoeren van aangiften zonder controles. In hoeverre voldoet de inzet van deze technologie aan de kaders van de gemeente Oss rondom de inzet van digitalisering?

Landelijk wordt veelvuldig gebruik gemaakt van tooling op het gebied van optische detectie van bouwmutaties. Deze tooling gebruikt AI om de optische herkenning in de software te verbeteren. Deze methode is reeds enkele jaren erg betrouwbaar gebleken en is daar mee beproefd. Om die reden promoot BSOB deze methode om bijvoorbeeld de aanwezigheid van zonnepanelen op daken te herkennen. De meeste deelnemers, waaronder gemeente Oss, geven opdracht aan marktpartijen om op deze wijze informatie in te winnen. BSOB is afnemer van de informatie die de gemeente Oss laat inwinnen. Dit leidt tot verbeteringen in het taxatiebestand van gemeente Oss. Voor zover deelnemers nog geen gebruik maken van deze methode, probeert BSOB de deelnemer te wijzen op het belang en efficiency van deze vorm van mutatiedetectie.

Vraag 2

En hoe verhoudt het digitaliseringsbeleid van BSOB zich in het algemeen ten aanzien van het digitaliseringsbeleid van alle deelnemers?

Het digitaliseringsbeleid van BSOB is vastgelegd in beleidsplannen die door het Dagelijks- en het Algemeen Bestuur van de GR worden goedgekeurd en in de Financiële verordening BSOB 2020. Onder dit beleid valt ook het al dan niet inzetten van AI (kunstmatige intelligentie) en het gebruik van cloud-technologie. Het digitaliseringsbeleid voldoet aan de geldende beveiligingseisen van BIG/BIWA. Dit wordt intern getoetst en het Dagelijks bestuur ziet toe op getrouwheid van de informatieverstrekking en de rechtmatigheid van de beheershandelingen. Zodat aan de eisen van rechtmatigheid, controle en verantwoording wordt voldaan. Voor de privacybescherming wordt o.a. jaarlijks het besluit gegevensverstrekking BSOB vastgesteld. Bepaalde gegevens mogen verstrekt worden aan expliciet genoemde bestuursorganen voor publiekrechtelijke taken. Deze lijst is limitatief

en opgenomen in het besluit. Gegevens worden alleen gedeeld na een schriftelijke aanvraag en na goedkeuring door de BSOB. Afhankelijk van de vraag wordt het verzoek overlegd met; de betrokkene, de toezichthouder van het Waterschap, de directeur van de BSOB, de Functionaris Gegevensbescherming van zowel de BSOB als de aanvrager en/of de Privacy Officer van zowel de BSOB als de aanvrager. Gegevens worden uitsluitend beveiligd verstrekt. Hierop wordt toegezien door de Privacy Officer, die hierover jaarlijks rapporteert aan het bestuur en door de externe accountant die hier jaarlijks een audit op uitvoert.

Vraag 3

Verder een opmerking over de flexibele schil voor het technische deel van informatieveiligheid. Deze flexibele schil is begrijpelijk. Maar we roepen wel op tot verhogen van bewustzijn van informatieveiligheid bij de eigen medewerkers omdat gebrek hieraan 1 van de grotere risico's is voor de organisatie.

Het inzetten van een flexibele schil is bedoeld ter uitbreiding van de capaciteit op het gebied van informatiebeveiliging en ter versterking van de Security Officer, die in vaste dienst van BSOB is. Hiermee wordt ook de kwetsbaarheid voor de organisatie beperkt bij uitval van deze medewerker.

Het verhogen van het bewustzijn voor informatiebeveiliging is een nadrukkelijk onderdeel van de inspanning die BSOB doet om in de tweede helft van 2025, waarbij met het aantonen van de opzet, het bestaan en de werking van de beheersmaatregelen op het gebied van informatiebeveiliging het door het Algemeen Bestuur gewenste volwassenheidsniveau 4 wordt gerealiseerd. Voor het vergroten van het bewustzijn van de medewerkers voor informatiebeveiliging wordt een uitgebreid pakket aan maatregelen uitgevoerd. Hierbij gaat het onder andere om:

- De inrichting van een speciale intranet pagina gericht op informatiebeveiliging, met informatie, instructies, tips en 'vraag-en-antwoord'
- Het regelmatig plaatsen van internetberichten waarin aandacht wordt besteed aan informatiebeveiligingsrisico's
- Het verstrekken van een wachtwoord-manager applicatie aan alle medewerkers
- Het dwingend opleggen van een zeer intensief e-learning programma voor alle medewerkers en een toetsing van het kennisniveau, waarover op medewerkersniveau wordt gerapporteerd aan het management van BSOB
- Het periodiek uitvoeren van zogenaamde 'phishing tests', waarbij getoetst wordt of medewerkers een risicovol mailbericht in voldoende mate herkennen en hierop op de juiste wijze reageren. Zij ontvangen hiervan een individuele terugkoppeling van de Security Officer. Over de uitkomsten van een dergelijke test wordt gerapporteerd aan het management
- Het regelmatig aandacht vragen voor informatiebeveiliging tijdens team- en afdelingsoverleggen

Brief aan gemeenteraad



- Het opstellen van werkinstructies voor de medewerkers voor inkomende telefoongesprekken en het verstrekken van privacy gevoelige informatie en de controle die hierop wordt uitgevoerd.

Ik hoop u met deze brief voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Frank den Brok
Wethouder Financiën