BINNENGEKOMEN
TEAM POSTBEHANDELING EN ARCHIVERING
D.D. 11-03-2025
No. 2025.00932
Portefeuillehouder: Fokke
Team: Team Functioneel Advies en Ondersteuning II

Aan het college van burgemeester en wethouders
Postbus 1992
6201BZ Maastricht

Maastricht, 11 maart 2025

Betreft: Schriftelijke vragen - Beveiligingsbeleid, informatievoorziening en device beperkingen voor raadsleden

Geachte college,

Als lid van de gemeenteraad hebben wij als raadsleden recht op volledige en onbelemmerde toegang tot informatie, zoals vastgelegd in artikel 169 lid 2 van de gemeentewet. Dit recht is essentieel om onze controlerende taak naar behoren uit te kunnen voeren. De gemeenteraad is immers het hoogste orgaan binnen de gemeente en moet onafhankelijk kunnen functioneren.

De gemeente Maastricht faciliteert dit door raadsleden te voorzien van een e-mailadres en een device (iPad) waarop alle benodigde informatie te vinden is. Hoewel dit op het eerste gezicht praktisch lijkt, roept de uitvoering van dit beleid bij mij ernstige vragen op over de toegankelijkheid, werkbaarheid en privacy.

Allereerst valt op dat de beveiligingsmaatregelen rondom het e-mailadres zeer complex zijn ingericht. Zo moet het wachtwoord iedere zes weken gewijzigd worden via een ingewikkeld proces waarbij gebruik moet worden gemaakt van drie verschillende apps, die allemaal op hetzelfde device staan. Dit proces is zo gecompliceerd dat het vrijwel onmogelijk is om zonder technische achtergrond fouten te vermijden, wat leidt tot blokkades van het email account. Deze wachtwoord procedures beperken de effectieve toegang tot gemeentelijke informatie en belemmeren ons werk als raadsleden.

Opmerkelijk is dat alle e-mail van de gemeenteraad via een aparte server loopt, welke gescheiden is van de rest van de gemeentelijke e-mailcorrespondentie. In theorie zou dit de beveiliging juist eenvoudiger moeten maken, aangezien deze mails zijn afgeschermd van de overige gemeentelijke systemen. Dit roept de vraag op waarom er desondanks is gekozen voor een dusdanig complex wachtwoord beleid.

Daarnaast is het uitsluitend toegestaan het verstrekte device (iPad) te gebruiken voor toegang tot gemeentelijke informatie. Het gebruik van privé-devices, zoals een laptop, is niet toegestaan. Dit beperkt mijn vrijheid om te werken op een manier die voor mij efficiënt en productief is. Een iPad werkt namelijk met een ander besturingssysteem dan een laptop, en dit verschil in functionaliteit maakt het voor mij moeilijker om mijn werk als raadslid goed uit te voeren.

Daarbij komt dat het gebruik van het verstrekte device voor privé-doeleinden wél is toegestaan. Dit roept vragen op over de privacy van raadsleden, omdat dit impliceert dat de gemeente mogelijk toegang heeft tot privé-gegevens die zich op dat device bevinden. Dit is een ongewenste situatie

waarin de controleur (de gemeenteraad) gecontroleerd kan worden door diegene die hij juist moet controleren (de gemeente).

Tot slot is recentelijk een nieuwe AI-functionaliteit geïntroduceerd via de Windows-app Pilot. Bij het inloggen verschijnt een melding dat informatie gedeeld wordt met de gemeente. Dit roept serieuze vragen op over welke gegevens precies worden gedeeld, met welk doel, en hoe dit zich verhoudt tot de privacy van raadsleden.

Om deze zorgen te adresseren, stel ik de volgende vragen.

1. Wat is de reden voor de huidige frequentie van wachtwoord wijzigingen (elke zes weken) voor raadsleden?
2. Welke risicoanalyse ligt ten grondslag aan deze maatregel, en waarom is gekozen voor deze specifieke beveiligingsstrategie?
3. Waarom is ervoor gekozen om het wachtwoord reset proces zo complex in te richten met drie verschillende apps?
4. Klopt het dat alle e-mail van de gemeenteraad via een aparte server loopt, welke gescheiden is van de rest van de gemeentelijke e-mailcorrespondentie? Zo ja, waarom is er desondanks gekozen voor een dergelijke complexiteit in het wachtwoord beleid, terwijl een aparte server juist eenvoudiger beveiligd zou kunnen worden?
5. Is het mogelijk de complexiteit van het reset proces te vereenvoudigen zonder de veiligheid in gevaar te brengen?
6. Waarom is het gebruik van privé-devices, zoals laptops, voor raadsleden niet toegestaan?
7. Op welke wijze is bij deze keuze rekening gehouden met de voorkeuren en werkwijze van raadsleden, zoals het gebruik van een laptop in plaats van een iPad?
8. Is het college bereid het beleid te heroverwegen en eventueel aan te passen zodat raadsleden de keuzevrijheid hebben met een ander apparaat te werken, mits dit veilig kan worden ingericht?
9. Hoe wordt de privacy van raadsleden gewaarborgd nu het device ook voor privé-doeleinden gebruikt mag worden?
10. Welke toegang heeft de gemeente tot de gegevens op deze devices, zowel voor gemeentelijke als voor privé-gebruik?
11. Hoe wordt gegarandeerd dat privé-gegevens niet door de gemeente kunnen worden ingezien of opgeslagen?
12. Waarom wordt er bij het inloggen op de AI-applicatie (via Pilot) aangegeven dat informatie met de gemeente gedeeld wordt?
13. Welke gegevens worden precies gedeeld en met welk doel?
14. Op welke wijze is de gemeenteraad betrokken geweest bij de keuze en implementatie van deze AI-functionaliteiten?
15. Hoe waarborgt het college de onafhankelijke toegang tot informatie voor raadsleden, gezien de huidige beveiligingsmaatregelen?
16. Welke stappen worden ondernomen om het beveiligingsbeleid te evalueren en te optimaliseren voor gebruiksvriendelijkheid zonder in te boeten op veiligheid?

Gezien de belangrijke rol van de gemeenteraad als hoogste orgaan binnen de gemeente en het fundamentele recht op onbelemmerde informatievoorziening, verzoek ik u deze vragen zorgvuldig en volledig te beantwoorden.

Hoogachtend, namens Partij Veilig Maastricht.

René Betsch
John Voorst
Pascal Ruijters