Gemeente Utrecht

BEANTWOORDING SCHRIFTELIJKE RAADSVRAGEN 2025, NUMMER 190

Datum	27 januari 2026
Van	College B&W
Behandeld door	Thomas Kruse
E-mailadres	t.kruse@utrecht.nl
Kenmerk	34063455
Beleidsveld	Personeel en Organisatie

Geachte leden van de raad,

Hierbij ontvangt u de beantwoording van de schriftelijke raadsvragen jaargang 2025 nummer 190 van Stevie Nolten en Noura Oul Fakir (BIJ1),Pepijn Zwanenberg en Hanane Bittich (LINK) van 13 november 2025 over Overname Zivver.
De gestelde vragen zijn onderaan bijgevoegd.

Vraag 1
Was de gemeente Utrecht op de hoogte van de overname van Zivver door Kiteworks?
Antwoord 1
Ja. We weten dit sinds juni 2025. We hebben hierover ook mondelinge vragen beantwoord op 26 juni. We hebben na deze beantwoording juridische en technische onderzoekslijnen uitgezet.

Vraag 2
Is er een risico-inschatting gemaakt over mogelijke gegevensbescherming onder buitenlandse wetgeving (bijv. CLOUD Act) nu gegevens via Zivver/Kiteworks verwerkt kunnen worden?
Antwoord 2
Ja, nadat de overname bij ons bekend was, hebben we een voorlopige risico-inschatting gemaakt. Wij hebben hierbij het risico als beperkt beoordeeld. Nu Zivver met de overname door Kiteworks onder Amerikaans eigenaarschap valt, betekent dat ook Amerikaanse wetgeving, zoals de Cloud Act, van toepassing kan zijn. Het risico dat de Amerikaanse autoriteiten werkelijk de gegevens kunnen vorderen wordt als beperkt ingeschat, omdat Zivver/Kiteworks gebruik maakt van geavanceerde versleuteling en onze contractuele afspraken met Zivver/Kiteworks toegang beletten. Daarbij zijn de sleutels niet in handen van Zivver/Kiteworks.

Vraag 3
Hoe past de overname in het bredere beleid van Utrecht rond digitale soevereiniteit, privacy en cybersecurity?
Antwoord 3
De overname staat op gespannen voet met onze wens om onafhankelijker te worden van Amerikaanse IT producten. Echter, de overname van Zivver speelde zich af voordat we ons beleid rond cloud op de geopolitieke ontwikkelingen hebben herijkt. De huidige DPIA, waarin we de privacy risico's in kaart brengen, gaan we vernieuwen. In de vernieuwde DPIA nemen we de overname van Zivver mee in de risicobeoordeling.

Vraag 4
Welke contractuele waarborgen bestaan er tussen de gemeente Utrecht en leveranciers als Zivver met betrekking tot wie toegang heeft tot versleutelde data, en welke audits of controles zijn daarin vastgelegd?
Antwoord 4
Leveranciers van de gemeente Utrecht worden gehouden aan meerdere contractuele waarborgen zoals de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) en de VNG-verwerkersovereenkomst voor de verwerking van persoonsgegevens, deze blijven onverminderd van kracht na de overname. Met Zivver hebben we concreet afgesproken dat zij moeten meewerken aan audits, maar dat onafhankelijke certificeringen die het beveiligingsniveau aantonen ook voldoende kunnen zijn. Zie verder het antwoord op vraag 5.

Vraag 5
Hoe waarborgt Utrecht dat gevoelige persoonsgegevens (zoals overheidscommunicatie.) die via platforms zoals Zivver worden verzonden, echt niet door derden kunnen worden ingezien, inclusief het moederbedrijf of buitenlandse autoriteiten?
Antwoord 5
Voor verwerkers van gevoelige persoonsgegevens, zoals Zivver, vragen wij dat ze aan bepaalde informatiebeveiligingsnormen voldoen. Zivver voldoet aan de ISO27001 en de NEN7510, zoals door onafhankelijke certificeringsinstellingen verklaard is.

Vraag 6
Hoe is de transparantie over het feit dat berichten “in platte leesbare vorm” verstuurd kunnen worden vóór encryptie? Is de gemeente geïnformeerd over deze werkwijze? Zo ja: wat is het oordeel van de gemeente daarover?
Antwoord 6
Ja, wij zijn hiervan op de hoogte. Zivver past op meerdere manieren encryptie toe, waaronder tijdens verzending en op opgeslagen berichten. Enkel door de toepassing van Data Loss Prevention (DLP) heeft Zivver tijdens het opstellen van mails een korte periode toegang tot de platte leesbare vorm. DLP is een maatregel die helpt voorkomen dat gevoelige informatie verkeerd verzonden wordt, waardoor datalekken kunnen worden voorkomen. Zodra de mail verzonden en opgeslagen wordt, heeft Zivver geen toegang tot de inhoud van de berichten. Berichten zijn dan volledig versleuteld en alleen wijzelf hebben toegang tot de encryptiesleutel om de inhoud van berichten te kunnen lezen.

Zo ja: wat is het oordeel van de gemeente daarover?
Op 22 september heeft de Informatiebeveiligingsdienst (IBD) van de VNG geconcludeerd dat risico’s rond de beschikbaarheid van Zivver licht zijn toegenomen, risico’s rond vertrouwelijkheid nagenoeg gelijk zijn gebleven en risico’s rond integriteit ongewijzigd zijn. Het risico voor de beschikbaarheid van Zivver is licht toegenomen, omdat een risico bestaat dat de Amerikaanse overheid via Kiteworks de toegang tot Zivver uitschakelt. Het IBD heeft de kans hierop als laag beoordeeld. We volgen de beoordeling van de IBD hierin en herzien risicoafwegingen wanneer situaties veranderen.

Vraag 7
Welke alternatieven heeft Utrecht overwogen voor Zivver en hoe wegen die kosten versus risico's?
Antwoord 7
We hebben in 2024 aanbesteed. Daarbij hebben we een zorgvuldig programma van eisen opgesteld en gehanteerd. Dit bevatte strikte criteria voor informatiebeveiliging, privacy, compliance, kosten en gebruiksvriendelijkheid.
Op basis hiervan is Zivver als beste uit de aanbesteding gekomen voor veilige communicatie binnen en buiten onze organisatie.
We hebben na de overname diverse gesprekken gevoerd met Zivver en intern onderzoek gedaan naar de risico’s van de overname zoals hierboven beschreven. In voorbereiding op de volgende aanbesteding zullen wij opnieuw onderzoeken welke leveranciers het beste aansluiten bij onze wensen en eisen voor veilige communicatie. Zie verder de beantwoording bij vraag 12.

Vraag 8
Is het college op de hoogte van de achtergrond van de huidige leiding van Kiteworks, waaronder hun voormalige functies binnen de Israëlische inlichtingendiensten?
Antwoord 8
Ja we zijn hiermee bekend. Wij toetsen niet op herkomst of nationaliteit van het management, maar vertalen het naar concrete risico-indicatoren in onze leveranciers- en ketenrisicobeoordeling.

Vraag 9
Welke risico's ziet het college in het toevertrouwen van vertrouwelijke gemeentelijke en persoonlijke gegevens aan een bedrijf waarvan de leidinggevende ervaring heeft binnen buitenlandse inlichtingendiensten?
Antwoord 9
Hiervoor verwijzen wij naar de beoordeling die het Rijk heeft gedaan, zoals verwoord in antwoorden op Kamervragen over Zivver[OBJ]er nu [OBJ]antwoorden op Kamervragen over Zivver[OBJ], namelijk dat er nu geen aanleiding is om aan te nemen dat de voormalige werkzaamheden bij buitenlandse inlichtingendiensten van een leidinggevende bij Kiteworks extra risico's oplevert. Wij blijven ook zelf deze risico's monitoren en op basis daarvan treffen wij, indien nodig, passende maatregelen.

Vraag 10
Kan het college bevestigen dat Utrecht voldoet aan de internationale verplichtingen rond mensenrechten en non-complicity (geen medeverantwoordelijkheid voor mensenrechtenschendingen), als het gaat om het gebruik van diensten van bedrijven met deze achtergrond? Hoe verhoudt dit zich tot de ambities van Utrecht op het gebied van digitale soevereiniteit, ethisch verantwoord ondernemen en mensenrechtenbeleid?
Antwoord 10
We voldoen bij nieuwe overeenkomsten aan de internationale verplichtingen door de volgende bepalingen standaard op te nemen in de aanbestedingen die vallen binnen de door het Rijk vastgestelde risicocategorieën, waaronder ICT (voornamelijk hardware):

1. Internationale Sociale Voorwaarden (ISV) Voor opdrachten boven de Europese aanbestedingsdrempel die vallen binnen de door het Rijk vastgestelde risicocategorieën gelden de actuele ISV-bestekteksten. Deze zijn bindend en geven concreet invulling aan de naleving van de Mensenrechtenbepaling, met aandacht voor due diligence, risicomanagement en rapportage.
2. Algemene Mensenrechtenbepaling VNG. Deze bepaling geldt als kapstok en verplicht opdrachtnemers zich in algemene zin te houden aan een proces tot het borgen van fundamentele mensenrechtennormen. Niet-naleving wordt aangemerkt als een toerekenbare tekortkoming in de nakoming van de overeenkomst.

Als tijdens de contractfase niet-naleving wordt vastgesteld, dan kan worden overgegaan tot het vorderen van de naleving van het contract en in het uiterste geval ontbinding van het contract.

Vraag 11
Vindt het college het wenselijk dat een gemeente die zich profileert als mensenrechtenstad, gevoelige communicatie onderbrengt bij een bedrijf met leiding uit een land dat beschuldigd wordt van grove mensenrechtenschendingen?
Antwoord 11
Als mensenrechtenstad streven wij er uiteraard naar om niet direct of indirect bij te dragen aan mensenrechtenschendingen. Om dit op een nog betere manier te kunnen doen zijn we momenteel bezig met een organisatiebreed handelingsperspectief mensenrechten, om zo deze keuzes helder en transparant te kunnen blijven maken. Hierover wordt u in Q1 geïnformeerd.

Vraag 12
Is het college bereid alternatieven te onderzoeken die beter aansluiten bij Europese waarden en mensenrechtennormen?
Antwoord 12
In voorbereiding op een volgende aanbesteding zijn wij bereid om alternatieven te onderzoeken en om ons programma van eisen opnieuw tegen het licht te houden. De eerste mogelijkheid om van

leverancier te wisselen zal juni 2027 zijn. Eind dit jaar zullen wij beoordelen of het nodig is om opnieuw aan te besteden of dat het contract met 1 jaar verlengd zal worden.

Hoogachtend
Burgemeester en wethouders van Utrecht,

de secretaris, de burgemeester,

Schriftelijke vragen: Overname Zivver

13 november 2025

Recent is in Follow the Money berichtgeving verschenen over de overname van het Nederlandse bedrijf Zivver door het Amerikaanse/Israëlische bedrijf Kiteworks. Zivver levert beveiligde communicatie oplossingen die ook door Nederlandse gemeenten, zorginstellingen en andere organisaties gebruikt worden om zeer gevoelige gegevens (waaronder medische en juridische informatie) te verzenden. Ook de gemeente Utrecht maakt gebruik van deze diensten.

Uit het artikel blijkt dat er aanzienlijke risico's bestaan rondom de bescherming van deze vertrouwelijke gegevens. Zo zou de beveiliging niet altijd end-to-end zijn, waardoor berichten in platte tekst door de dienstverlener verwerkt kunnen worden. Daarnaast roept de overname door een buitenlands bedrijf vragen op over toegang tot data door buitenlandse overheden, en de juridische en politieke context waarin deze onderneming opereert.
Extra zorgelijk is dat de leiding van Kiteworks bestaat uit personen met een achtergrond in de Israëlische inlichtingendiensten. Dit geeft, mede gezien de internationale context van mensenrechtenschendingen en genocide door Israël, aanleiding tot zorgen over de integriteit, onafhankelijkheid en veiligheid van de dienstverlening.

Gezien het belang van digitale soevereiniteit, gegevensbescherming en de voorbeeldfunctie die de gemeente Utrecht als mensenrechtenstad wil vervullen, stellen de fracties van BIJ1 en LINK de volgende vragen:

Vragen:

1. Wist het gemeentebestuur of de gemeentelijke organisatie van Utrecht van de overname van Zivver door Kiteworks?

2. Zo ja, is er een risico-inschatting gemaakt van mogelijke gegevensbescherming onder buitenlandse wetgeving, nu gegevens via Zivver/Kiteworks verwerkt en opgeslagen kunnen worden?

3. Hoe past deze overname in het bredere beleid van de gemeente Utrecht ten aanzien van digitale soevereiniteit, privacybescherming en cybersecurity?

4. Welke contractuele waarborgen bestaan er tussen de gemeente Utrecht en leveranciers als Zivver met betrekking tot wie toegang heeft tot versleutelde data, en welke audits of controles zijn daarin vastgelegd?

5. Hoe waarborgt Utrecht dat gevoelige persoonsgegevens (zoals overheidscommunicatie.) die via platforms zoals Zivver worden verzonden, echt niet door derden kunnen worden ingezien, inclusief het moederbedrijf of buitenlandse autoriteiten?

6. Hoe is de transparantie over het feit dat berichten “in platte leesbare vorm” verstuurd kunnen worden vóór encryptie? Is de gemeente geïnformeerd over deze werkwijze? Zo ja: wat is het oordeel van de gemeente daarover?

7. Welke alternatieven heeft Utrecht overwogen voor Zivver en hoe wegen die kosten versus risico's?

8. Is het college op de hoogte van de achtergrond van de huidige leiding van Kiteworks, waaronder hun voormalige functies binnen de Israëlische inlichtingendiensten?

9. Welke risico’s ziet het college in het toevertrouwen van vertrouwelijke gemeentelijke en persoonlijke gegevens aan een bedrijf waarvan de leidinggevende ervaring heeft binnen buitenlandse inlichtingendiensten?

10. Kan het college bevestigen dat Utrecht voldoet aan de internationale verplichtingen rond mensenrechten en non-complicity (geen medeverantwoordelijkheid voor mensenrechtenschendingen), als het gaat om het gebruik van diensten van bedrijven met deze achtergrond? Hoe verhoudt dit zich tot de ambities van Utrecht op het gebied van digitale soevereiniteit, ethisch verantwoord ondernemen en mensenrechtenbeleid?

11. Vindt het college het wenselijk dat een gemeente die zich profileert als mensenrechtenstad, gevoelige communicatie onderbrengt bij een bedrijf met leiding uit een land dat beschuldigd wordt van grove mensenrechtenschendingen?

12. Is het college bereid alternatieven te onderzoeken die beter aansluiten bij Europese waarden en mensenrechtennormen?

Ingediend door:

- Stevie Nolten en Noura Oul Fakir, BIJ1
- Pepijn Zwanenberg en Hanane Bittich, LINK