

Detailrapport Vraag en antwoord los v/h Raadsplein (ID 1071)

Veld	Waarde
Datum vraag	23-08-2026
Onderwerp	Informatiebeveiliging, autorisatiebeheer en beveiligingsincident Woo-dossier
Fractie(s)	LEV
Vraag en antwoord	Op 12 augustus 2026 heeft de gemeente een inwoner schriftelijk geïnformeerd over een beveiligingsincident rond een Woo-dossier. In deze brief wordt vermeld dat in juli en augustus mogelijk te veel medewerkers toegang hadden tot het betreffende Woo-dossier en dat daarbij persoonsgegevens, waaronder NAW-gegevens, geboortedatum, BSN en contactgegevens, mogelijk voor te veel medewerkers inzichtelijk zijn geweest. De gemeente kwalificeerde dit als een beveiligingsincident/datalek, beperkte vervolgens de toegang tot het Woo-dossier, legde het incident vast in het interne datalekregister en meldde het datalek bij de Autoriteit Persoonsgegevens. Op 18 augustus 2026 heeft de gemeente de eerdere melding over het datalek ingetrokken. Volgens het vervolgonderzoek zouden alleen medewerkers het dossier daadwerkelijk hebben geraadpleegd die betrokken waren bij de behandeling van het Woo-verzoek. Tegelijkertijd wordt in dezelfde brief bevestigd dat de eerder te brede toegang tot het dossier in het interne datalekregister vastgelegd blijft en dat de toegang tot het Woo-dossier is beperkt. Naar aanleiding hiervan heeft de fractie van Lokaal Edam-Volendam vragen over de inrichting en werking van het autorisatiebeheer, de informatiebeveiliging en de interne beheersing rond Woo-dossiers. Deze vragen zijn nadrukkelijk gericht op het functioneren van het gemeentelijke systeem en de bestuurlijke verantwoordelijkheid daarvoor, en niet op openbaarmaking van persoonsgegevens van individuele medewerkers. Vraag 1. Kan het college toelichten wat op 12 augustus 2026 feitelijk was vastgesteld waardoor de situatie door de gemeente werd gekwalificeerd als een beveiligingsincident/datalek? Antwoord 1: Op 12 augustus 2026 was vastgesteld dat het betreffende Woo-dossier via de reguliere autorisaties in het zaakstelsel toegankelijk was voor alle accounts met systeemtoegang. Omdat daarbij persoonsgegevens in het dossier konden worden geraadpleegd, is de situatie destijds als een mogelijk beveiligingsincident en voorlopig datalek 'met een hoog risico voor betrokkenen'

	beoordeeld. Vraag 2. Hoeveel gebruikersaccounts konden voor het beperken van de toegang technisch toegang verkrijgen tot het betreffende Woo-dossier, ongeacht of uit logging blijkt dat zij het dossier daadwerkelijk hebben geopend? Antwoord 2: Alle gebruikersaccounts met toegang tot het zaaksysteem konden technisch toegang verkrijgen tot het betreffende Woo-dossier. Vraag 3. Hoeveel gebruikersaccounts beschikken na de getroffen beveiligingsmaatregel nog over toegang tot het betreffende dossier? Antwoord 3: Nog steeds alle gebruikersaccounts met toegang tot het zaaksysteem. Vraag 4. Op basis van welke rollen, functies of functionele categorieën werd voor 12 augustus toegang tot Woo-dossiers verleend? Antwoord 4: De toegang op Woo-dossiers is niet beperkt op basis van specifieke rollen, functies of functionele categorieën. De toegang volgde in dit geval uit de brede systeemautorisaties binnen het zaaksysteem. Vraag 5. Was de toegang voor de getroffen maatregel ingericht volgens het beginsel dat uitsluitend medewerkers die deze toegang voor hun werkzaamheden noodzakelijk hebben toegang krijgen tot de betreffende persoonsgegevens? Antwoord 5: Nee. Vraag 6. Zo ja, hoe verklaart het college dan dat op 12 augustus schriftelijk is meegedeeld dat mogelijk te veel medewerkers toegang hadden en dat vervolgens de toegang tot het dossier daadwerkelijk is beperkt? Antwoord 6: De schriftelijke melding op 12 augustus was gebaseerd op een voorlopige risicobeoordeling. Daarbij is uitgegaan van het feit dat het dossier toegankelijk was binnen de brede systeemautorisatie. Een beperking van de toegang is overwogen, echter na afronding van een onderzoek, is gebleken dat een beperking niet nodig was. Vraag 7. Wat is tussen 12 en 18 augustus uit het vervolgonderzoek naar voren gekomen waardoor de gemeente tot de conclusie is gekomen dat de eerdere melding kon worden ingetrokken? Antwoord 7:
--	---

	Uit vervolgonderzoek, waaronder de analyse van logging en autorisatiegegevens, is gebleken dat geen aanwijzingen zijn gevonden dat medewerkers buiten de betrokken behandelaars het dossier daadwerkelijk hebben geopend of ingezien. Op basis daarvan is de voorlopige melding ingetrokken. Vraag 8. Maakt het college bij deze conclusie onderscheid tussen ongeautoriseerde daadwerkelijke inzage en het beschikbaar/toegankelijk zijn van persoonsgegevens voor medewerkers voor wie deze toegang niet noodzakelijk was? Zo ja, kan het college dit onderscheid en de gevolgen daarvan voor de beoordeling van het beveiligingsincident toelichten? Antwoord 8: Ja. Er is onderscheid tussen daadwerkelijke inzage en het technisch toegankelijk zijn van een dossier binnen het zaaksysteem. In dit geval was het dossier technisch toegankelijk voor alle accounts met systeemtoegang, maar uit onderzoek is gebleken dat alleen bevoegde medewerkers het dossier daadwerkelijk hebben ingezien. De intrekking van de melding ziet op dat laatste. Vraag 9. Waarom blijft de eerder te brede toegang als datalek in het interne datalekregister geregistreerd wanneer de melding van het datalek tegelijkertijd is ingetrokken? Antwoord 9: Het interne register legt de volledige incidentafhandeling vast, inclusief de eerste beoordeling, het vervolgonderzoek en de uiteindelijke conclusie. Daarom blijft de oorspronkelijke constatering administratief zichtbaar, ook als de voorlopige melding later is ingetrokken. Vraag 10. Is de oorspronkelijke melding bij de Autoriteit Persoonsgegevens daadwerkelijk ingetrokken of gewijzigd? Zo ja, op welke datum en op basis van welke nieuwe feiten? Antwoord 10: Ja, de oorspronkelijke voorlopige melding is gedaan op 6 augustus 2026 en op 17 augustus ingetrokken na het vervolgonderzoek, op basis van de bevinding dat geen aanwijzingen zijn gevonden voor daadwerkelijke onbevoegde inzage. Vraag 11. Is de Functionaris Gegevensbescherming voorafgaand aan de oorspronkelijke melding, de beperking van de toegangsrechten en/of de latere intrekking geraadpleegd? Zo ja, heeft de FG hierover een zelfstandig advies uitgebracht? Antwoord 11: Nee, de Functionaris Gegevensbescherming is in deze fase niet vooraf geraadpleegd.
--	--

	Vraag 12. Is de CISO betrokken geweest bij de beoordeling van het incident, de analyse van het autorisatiemodel en de getroffen beveiligingsmaatregelen? Zo ja, heeft de CISO hierover schriftelijk geadviseerd? Antwoord 12: Ja, de CISO is betrokken geweest bij de beoordeling van het incident, de analyse van het autorisatiemodel en de getroffen maatregelen, en heeft hierover geadviseerd. Vraag 13. Heeft naar aanleiding van dit incident een bredere controle plaatsgevonden op autorisaties van andere Woo-dossiers, teneinde vast te stellen of dezelfde toegangsstructuur daar eveneens werd of wordt toegepast? Zo ja, wat is daarvan de uitkomst? Zo nee, waarom niet? Antwoord 13: Nee, er heeft geen bredere controle op andere Woo-dossiers plaatsgevonden. Daar was op dit moment geen aanleiding voor binnen de incidentafhandeling. Vraag 14. Sinds wanneer bestond de inmiddels aangepaste toegangsstructuur voor Woo-dossiers en is onderzocht of gedurende die periode persoonsgegevens in andere Woo-dossiers toegankelijk zijn geweest voor meer medewerkers dan noodzakelijk? Antwoord 14: De toegangsstructuur bestond al jaren en is onderdeel van de generieke inrichting van het zaakstelsel. Er is niet afzonderlijk onderzocht of in andere Woo-dossiers gedurende die periode vergelijkbare toegang bestond. Vraag 15. Worden toegangsrechten tot Woo-dossiers periodiek gecontroleerd en vindt daarbij aantoonbaar controle plaats op daadwerkelijke noodzaak, functiescheiding en het need-to-know-beginsel? Antwoord 15: Nee, niet op die manier. Periodieke controle op individuele noodzaak en need-to-know is voor Woo-dossiers niet structureel ingericht. Vraag 16. Heeft het college naar aanleiding van dit incident vastgesteld dat de inrichting van het autorisatiebeheer voor Woo-dossiers voldoet aan de AVG, het gemeentelijke informatiebeveiligingsbeleid en de voor gemeenten geldende informatiebeveiligingskaders? Zo ja, op basis van welk onderzoek of advies? Antwoord 16: Nee. Dit incident is niet de aanleiding geweest voor deze beoordeling. De informatiebeveiligingskaders en het autorisatiebeheer voor Woo-dossiers werden al betrokken in het
--	---

	lopende traject voor de vervanging van het huidige zaaksysteem. In het kader van dat traject worden de relevante eisen en kaders nadrukkelijk meegenomen bij de inkoop en verdere inrichting. Het incident bevestigt het belang van deze reeds geplande aandachtspunten. Vraag 17. Is dit incident, inclusief de oorspronkelijke constatering, de getroffen maatregel en de latere intrekking, gemeld of gerapporteerd binnen de reguliere bestuurlijke informatiebeveiligingsrapportages? Zo nee, waarom niet? Antwoord 17: Het incident is intern geregistreerd en operationeel afgehandeld. Vraag 18. Kan het college de gemeenteraad informeren of in de afgelopen drie jaar andere incidenten zijn geregistreerd waarbij sprake was van te ruime autorisaties tot dossiers of persoonsgegevens, zonder daarbij persoonsgegevens of beveiligingsgevoelige technische details openbaar te maken? Antwoord 18: Zie beantwoording op eerdere vragen. Vraag 19. Is het college bereid de raad, zo nodig onder geheimhouding, inzage te verschaffen in de relevante bevindingen van het interne onderzoek en de adviezen van FG en/of CISO, zodat de raad kan controleren of de inmiddels getroffen maatregelen afdoende zijn? Antwoord 19: De relevante bevindingen zijn in de beantwoording van deze gestelde vragen gedeeld.
Bijlage(s)	IMG_0850 (2) IMG_0851 IMG_0852 IMG_0853 IMG_0854 IMG_0855 IMG_0856 IMG_1023 IMG_1024 IMG_1025 IMG_1026 IMG_1027