

**Woo-verzoek 01042026 Betreft: Uitgebreid Woo-verzoek '5.1.2e':
(Cyber)weerbaarheid, (integrale) veiligheid, ondermijning, datalekken en
bescherming van de rechtsstaat (2021-2026)**

Op grond van de Wet open overheid (Woo) verzoek ik u om openbaarmaking van de onderstaande documenten en informatie. Dit verzoek is een **uitdrukkelijke aanvulling en uitbreiding** op mijn eerdere verzoek d.d. 3 december 2025 (link: <https://open.gelderland.nl/woo-documenten/woo-deelbesluit-2-over-ai-en-privacyvraagstukken2025-014393-rol-en-bevoegdheden-fg-and-werkwijze-privacyvraagstukken> (kenmerk 2025-014393)). In 2021 was er bij Provincie Gelderland een groot datalek/incident bij Provincie Gelderland Gelderland (link: [Provincie Gelderland is slachtoffer geworden van hack | Tech | NU.nl](#)). Helaas lijkt het op dit moment niet (veel) beter te zijn en/of zelfs slechter gesteld met de (cyber)weerbaarheid van Provincie Gelderland zelf. Ondertussen gaat de digitalisering met o.a. de digitale identiteit, Digital Decade EU, AI(-verordening) etc. in volle vaart door bij Provincie Gelderland waar ik o.a. in 2024 een bijdrage over had bij Provinciale Staten Gelderland op de Wet gegevensverwerking door Samenwerkingsverbanden (WSD), ondermijning, etc. (link: **5.1.2e**).

Ik wil hiermee transparantie verkrijgen over hoe fundamentele grond- en mensenrechten van burgers worden geborgd. Zeker na de datalekken/cyberaanvallen in 2026 waarbij allerlei overheidsinstanties verantwoordelijkheid proberen te ontlopen/verdoezelen. Mijn Woo-verzoek bestaat uit de volgende hoofdpunten:

1. Bestrijding 'ondermijning' en samenwerkingsverbanden (WGS/WODG/etc)

- a. Documenten, convenanten, risicobeoordelingen en communicatie waarin de rol van de Provincie Gelderland is vastgelegd binnen de **Wet Gegevensverwerking door Samenwerkingsverbanden (WGS)**. Wie is verantwoordelijk als er iets mis gaat?
- b. Informatie over de uitvoering van de (aankomende) **Wet op de defensiegereedheid (WODG)** en vergelijkbare wetten en de impact hiervan op de privacy van Gelderlanders.
- c. Overzicht van interne en externe partijen waarmee persoonsgegevens worden gedeeld in het kader van ondermijningsbestrijding, inclusief de bijbehorende 'checks and balances' en andere manieren van controles/evaluaties.
- d. Documentatie over gebruikte (AI-)technologieën, algoritmes en software (zoals Palantir) bij deze samenwerkingen. Ik verzoek om aanbestedingen, DPIA's, verwerkersovereenkomsten en evaluaties die aantonen hoe een 'Toeslagenaffaire 2.0' én Chinese controlestaat wordt voorkomen. Ook wat de plannen t/m 2030 zijn.

2. Privacy en Informatiebeveiliging (AVG/BIO/NIS2/WPG)

- a. Een volledig overzicht van datalekken, incidenten, cyberaanvallen, bezwaarschriften, klachten, meldingen etc. bij Provincie Gelderland sinds 2021, inclusief de

correspondentie hierover met de Autoriteit Persoonsgegevens en andere samenwerkingspartners. Zover mogelijk zo uitgebreid mogelijk over datalekken/cyberaanvallen in 2026 en de afhandeling en geleerde lessen hiervan.

b. Documenten waaruit de specifieke verantwoordelijkheden en aansprakelijkheden blijken van de (privacy-)organisatie van Provincie Gelderland bij calamiteiten, incidenten, cyberaanvallen, datalekken en hacks. Ook met evaluatie in 2025 en 2026.

c. Evaluaties en 'geleerde lessen' naar aanleiding van het datalek uit 2021. Specifiek verzoek ik om informatie over incidenten/datalekken op provinciale devices en/of prive devices waarop Provincie Gelderland via een Sharepoint en/of Microsoft Edge gekomen zou zijn met datalekken/verwijdering/wijziging tot gevolg in 2026 en de beoordeling daarvan door in ieder geval de FG en CISO. Ook graag een overzicht wie de (ingehuurde) FG van Provincie Gelderland is/was en wat daarvoor de prijs is/was in 2025 én 2026.

d. Informatie over de inzet van leveranciers zoals Microsoft (365, Azure, Intune etc), KPN en Odido, en de verdeling van aansprakelijkheid bij cyberaanvallen/datalekken/etc.

3. Provinciaal laptop (en -account) voor Statenleden, fractievolgers en medewerkers

a. Gebruikshandleidingen en instructies die Statenleden, fractievolgers en medewerkers ontvangen bij uitgifte van hardware (laptop/telefoon), specifiek over het (toegestane) privégebruik. Ook hoe ze een uitleg krijgen over hoe de laptop gebruikt kan worden.

b. De volledige lijst van logcategorieën die worden bijgehouden ter detectie van ongeautoriseerde toegang. Ook wie hierop controleert en evalueert.

c. Informatie over de technische mogelijkheid en/of uitvoering van het verwijderen/wijzigen/etc van documenten/e-mails op provinciale accounts of gekoppelde privé-accounts door beheerders. Ook of dit in 2025 en 2026 is gebeurd én waarom. Documentatie over het (mogelijke) monitoren van privé-activiteiten of privé-accounts op provinciale hardware dan wel prive devices door/via Provincie Gelderland.

d. Informatie over de cyberverzekeringen van de provincie en de dekking bij aansprakelijkheid door hacks/datalekken/cyberaanvallen etc.

Tijdsbestek en afhandeling

Dit verzoek ziet op de periode **1 januari 2021 tot en met de datum van uw besluit**. Gezien de relevantie voor de grond- en mensenrechten van burgers, verzoek ik u de wettelijke besluittermijn strikt te hanteren.

Graag ontvang ik op korte termijn een ontvangstbevestiging en een indicatie van de verdere procedure.

Hoogachtend,

5.1.2e