



gemeente  
**Zoetermeer**

**Aan**

De gemeenteraad van Zoetermeer

**Zaakid**

2026-072223

**Van**

Het college/ Wethouder Van der Meer

**Datum**

28 mei 2026

**Onderwerp**

Beantwoording van de schriftelijke vragen van de Zoetermeer  
Vooruit-fractie d.d. 8 mei 2026 over 'Risico's op datalekken en  
bescherming van persoonsgegevens'

**Bijlagen**

-

**Vraag 1**

Is het college bekend met de hack bij de gemeente Epe en de aard en omvang van het datalek?

**Antwoord 1**

Ja we zijn daarvan op de hoogte.

**Vraag 2**

In hoeverre zijn de ICT-systemen en databestanden van de gemeente Zoetermeer beschermd tegen vergelijkbare cyberaanvallen?

**Antwoord 2**

Wij beschermen onze systemen met een mix van preventieve informatiebeveiligingsoplossingen, inzet op kennis, houding en gedrag van onze medewerkers en we zetten in op 'geen toegang tenzij principes' om digitale inbraken te beperken.

We doen al het mogelijke om onze systemen te beschermen, maar gezien de wedloop met de digitale criminelen kunnen we nooit helemaal uitsluiten dat er iets misgaat.

Daarom hebben we continue monitoring ingeregeld om incidenten z.s.m. te ontdekken en te kunnen handelen om de gevolgen te beperken. Ook vindt jaarlijks (wettelijke) toetsing van onze systemen door professionele bedrijven plaats.

**Vraag 3**

Welke maatregelen heeft de gemeente Zoetermeer momenteel genomen om persoonsgegevens van inwoners te beschermen tegen datalekken en hacks?

**Antwoord 3**

Zie beantwoording van vraag 2. Daarnaast passen we principes van functiescheiding toe in onze applicaties, waarbij uitsluitend toegang tot systemen en informatie wordt toegekend als dit voor de werkzaamheden van de medewerker noodzakelijk is. We passen Multi Factor Authentication (MFA) toe wat betekent dat medewerkers hun identiteit meerdere malen bewijzen om in te loggen op gemeentelijke systemen. Informatie wordt bij voorkeur versleuteld opgeslagen. Informatiebeheer ziet toe op het voldoen aan bewaartermijnen. Dit borgt dat we geen data in onze systemen hebben die volgens de wettelijke bewaartermijnen al vernietigd hadden moeten zijn.

#### **Vraag 4**

Worden er binnen de gemeente Zoetermeer kopieën van identiteitsbewijzen (zoals paspoorten, rijbewijzen en ID-kaarten) opgeslagen? Zo ja, hoe worden deze beveiligd?

#### **Antwoord 4**

Wij vragen alleen om kopieën van identiteitsbewijzen in het proces van in dienst treden van medewerkers met een rechtstreeks dienstverband bij de gemeente Zoetermeer. Identiteitsbewijzen worden versleuteld opgeslagen en na verlopen van de wettelijke bewaartermijn verwijderd. Bij inhuur ligt deze verantwoordelijkheid bij de tussenpartij, (detacheerder, uitzendbureau). Voor wat betreft de opslag van de kopieën van identiteitsbewijzen zijn met onze partners juridische afspraken gemaakt in zowel contracten als verwerkingsovereenkomsten.

#### **Vraag 5**

Heeft de gemeente Zoetermeer recent onafhankelijke beveiligingsaudits of penetratietesten laten uitvoeren? Zo ja, wat waren de belangrijkste bevindingen?

#### **Antwoord 5**

We voeren jaarlijks een onafhankelijke penetratietest uit met een extern professioneel cybersecurity bedrijf. De meeste recente penetratietest is in december 2025 uitgevoerd. Hierin is ook Operationele Technologie (denk hierbij aan software in gemalen en dergelijke) meegenomen. De bevindingen zijn intern bekend en verbeteracties zijn opgepakt. Ingaan op de belangrijkste bevindingen in een openbare setting levert risico's op voor onze informatiebeveiliging.

Aanvullend op de jaarlijkse penetratietest maken we intern gebruik van een oplossing die continu onze IT-infrastructuur scant op (nieuwe) bekende kwetsbaarheden en ons helpt te focussen op de meeste risicovolle kwetsbaarheden in onze inspanning tot continue verhoging van onze informatiebeveiliging.

Daarnaast hebben we sinds 2024 ZeroDayZoetermeer waar we jaarlijks studenten van de Haagse Hogeschool onze systemen laten testen. De laatste editie heeft 8 mei 2026 plaats gevonden en leverde twee kwetsbaarheden op. Deze zijn opgepakt met de betrokken afdeling en verantwoordelijke leveranciers.

#### **Vraag 6**

Zijn er in de afgelopen jaren datalekken of cyberincidenten geweest binnen de gemeente Zoetermeer? Zo ja, wat was de aard en hoe zijn deze afgehandeld?

#### **Antwoord 6**

Datalekken komen ook bij de gemeente voor. Sommige daarvan worden verplicht op grond van de AVG binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens omdat deze een hoog risico zijn op de persoonlijke levenssfeer van inwoners zoals gevoelige informatie uit het Sociaal Domein. Andere datalekken hebben geen hoge risico's en worden intern opgeslagen en gerapporteerd.

Er hebben zich het afgelopen jaar geen cyberincidenten voorgedaan op de systemen van Zoetermeer. Volgens ons eigen protocol worden incidenten beoordeeld op impact. Op Cyberincidenten wordt altijd direct geacteerd om de oorzaak te achterhalen, de gevolgen vast te stellen en deze zo beperkt mogelijk te houden. Incidenten worden gemeld bij de bestuurder in de periodieke rapportage. In geval van een ernstig incident zal dit ook gemeld worden bij onze externe toezichthouder(s) (Nationaal Cyber Security Center (NCSC), Informatie Beveiligingsdienst (IBD))

**Vraag 7**

Welke protocollen zijn er in werking bij een (mogelijk) datalek om inwoners snel te informeren en te beschermen tegen misbruik van hun gegevens?

**Antwoord 7**

Er is een afzonderlijk proces ingericht voor datalekken met een bestuurlijk of politiek gevoelig karakter. Binnen dit proces is geborgd dat relevante sleutelfiguren tijdig worden geïnformeerd, waaronder de gemeentesecretaris, verantwoordelijk conerndirecteur, Functionaris Gegevensbescherming (FG), het college en voor zover nodig (in overleg met de sleutelfiguren) de gemeenteraad.

**Vraag 8**

Hoe wordt samengewerkt met landelijke instanties en cybersecurity-organisaties om digitale dreigingen te voorkomen en te bestrijden?

**Antwoord 8**

Wij werken onder andere samen met de gemeentes in veiligheidsregio Haaglanden en met VNG-IBD. Voorbeelden van beleid, informatie en kennis, worden gedeeld. We werken samen met onze eigen cybersecurity-partners op het gebied van toegepaste technologie, bewustwording, kennisverdieping en inkopen van dienstverlening.

Vanuit Privacy is een regionaal juristennetwerk geïnitieerd waarin periodiek overleg plaatsvindt over actuele privacy- en informatiebeveiligingsvraagstukken. Daarnaast wordt interdisciplinair (Informatiebeveiliging, Privacy en Informatiebeheer) actief kennis en expertise met elkaar gedeeld.

**Vraag 9**

Acht het college aanvullende maatregelen nodig naar aanleiding van de situatie in Epe? Zo ja, welke?

**Antwoord 9**

Wij zijn op de hoogte van de omstandigheden die hebben geleid tot de hack en het daaropvolgende datalek bij de gemeente Epe. Bepaalde maatregelen die de hack bij Epe hadden kunnen voorkomen, worden al toegepast bij Zoetermeer. Er is op dit moment geen directe aanleiding voor acuut ingrijpen naar aanleiding van het incident bij Epe.

**Vraag 10**

Op welke wijze worden inwoners geïnformeerd over hoe zij zelf hun persoonsgegevens kunnen beschermen tegen misbruik?

**Antwoord 10**

De gemeente organiseert, in het kader van het verhogen van de digitale veiligheid, bewustwordings-bijeenkomsten voor verschillende doelgroepen, zoals senioren, jongeren en ondernemers, om online criminaliteit te voorkomen. Het doel hiervan is om de weerbaarheid van inwoners te vergroten en (herhaald) slachtofferschap te voorkomen.

Voor technische vragen kunt u zich wenden tot:

Naam : Vincent Roos

Telefoonnummer : +31793469615

E-mailadres : v.m.roos@zoetermeer.nl