

Gemeenteraad Harderwijk
T.a.v. de fractie van de VVD
Postbus 149
3840 AC HARDERWIJK

datum: 24 juni 2026
ons kenmerk: 02430000255944 / 02430000886723
uw brief van: 23 april 2026
uw kenmerk:
onderwerp: Beantwoording schriftelijke vragen m.b.t. informatieveiligheid, preventie van datalekken en ClickFix-risico's

Geachte meneer Van Nieuwenhuizen,

Op 24 april 2026 zijn er namens uw fractie schriftelijke vragen ontvangen over informatieveiligheid, preventie van datalekken en ClickFix-risico's. Hieronder vind u de beantwoording op deze vragen. *Door een technische fout is deze beantwoording veel later bij u terecht gekomen dan de bedoeling was, onze excuses daarvoor.*

Vraag 1:

Heeft het college kennisgenomen van het grootschalige datalek bij de gemeente Epe, waarbij persoonsgegevens van nagenoeg alle inwoners zijn buitgemaakt?

Antwoord 1:

Ja, het college heeft met bezorgdheid kennisgenomen van de berichtgeving over het datalek bij onze buurgemeente Epe. Het incident onderstreept de voortdurende noodzaak voor alertheid op het gebied van informatiebeveiliging. Het bestuur is over de details van dit specifieke incident en de duiding daarvan door Meerinzicht geïnformeerd.

Vraag 2:

De gegevens in Epe zijn naar verluidt buitgemaakt via de zogenaamde ClickFix-methode (waarbij gebruikers worden verleid op kwaadaardige links te klikken onder het mom van browser-updates). Is de gemeente Harderwijk ook kwetsbaar voor een dergelijke methode? Zo ja, welke technische en procedurele maatregelen zijn er getroffen om dit specifiek te voorkomen?

organisatie eenheid: Domein Bedrijfsvoering
behandeld door: J.M. van Hoof
telefoonnummer: 085 1108 218
bijlage(n):

Havendam 56
Correspondentieadres:
Postbus 149
3840 AC Harderwijk
T 0341 411 911
E info@harderwijk.nl
W harderwijk.nl
B NL44 BNGH 0285 0033 13

Antwoord 2:

Hoewel absolute veiligheid in een continu veranderend dreigingslandschap niet bestaat, hanteert de gemeente Harderwijk (EHZM) een proactieve en meerlaagse beveiligingsstrategie. Wij worden door de Informatiebeveiligingsdienst (IBD) direct geïnformeerd over nieuwe aanvalsmethoden zoals 'ClickFix'.

Specifiek voor deze methode hebben wij technische barrières opgeworpen die het uitvoeren van onbekende scripts of systeemcommando's door gebruikers blokkeren. Mocht een incident onverhoopt toch plaatsvinden, dan zorgt onze netwerkarchitectuur ervoor dat de impact beperkt blijft en verdere verspreiding ('besmettingsgevaar') effectief wordt bemoeilijkt. Vanwege de veiligheid van onze systemen kunnen wij details over deze technische maatregelen niet openbaar delen. Naast techniek investeren we continu in de 'menselijke factor' via awarenessprogramma's, zodat medewerkers malafide verzoeken sneller herkennen.

Vraag 3:

Wordt er binnen de ambtelijke organisatie gewerkt met 'lijstwerk' (zoals Excel-bestanden of exports) waarin kritieke persoonsgegevens zoals BSN, geboortedatum en naam gelijktijdig buiten de beveiligde kernsystemen worden opgeslagen?

Antwoord 3:

Het college hecht grote waarde aan de zorgvuldige omgang met persoonsgegevens. Ons vigerende beleid is helder: privacygevoelige informatie hoort uitsluitend thuis in de daarvoor bestemde, beveiligde zaaksystemen. We herkennen echter de landelijke uitdaging dat 'lijstwerk' in de dagelijkse praktijk een risico kan vormen.

Wij werken momenteel aan het herstructureren en borgen van ons verwerkingenregister om nog scherper zicht te krijgen op informatiestromen. De signalen van de Functionaris Gegevensbescherming (FG) over het gebruik van bestanden buiten de kernsystemen nemen wij zeer serieus; dit is voor ons een belangrijk speerpunt in het verbeterplan informatiebeveiliging. De focus ligt hierbij op het minimaliseren van exports en het bieden van veilige alternatieven binnen de gecontroleerde omgeving.

Vraag 4:

Middels workspace-accounts is het mogelijk om eigen hardware te gebruiken (Bring Your Own Device - BYOD). Hoewel dit voordelig is voor de hardwarekosten en prettig voor de eindgebruiker, brengt dit extra veiligheidsrisico's met zich mee. Wat is de visie van het college op het gebruik van eigen hardware in relatie tot de informatiebeveiliging?

Antwoord 4:

Het college deelt de analyse dat het gebruik van eigen hardware (BYOD) extra risico's met zich meebrengt, aangezien de controle op de beveiligingsinstellingen van privétoestellen beperkt is. In het licht van de toenemende cyberdreigingen en de aankomende vervanging van hardware in 2026, heroverwegen wij onze visie.

Een te overwegen keuze is om over te stappen naar het principe 'Company Owned, Business Only' (COBO). Hiermee krijgt de gemeente de volledige regie over de beveiliging van de apparatuur en borgen we een strikte scheiding tussen privé- en zakelijke data. Vooruitlopend hierop worden medewerkers strikt geïnstrueerd om uitsluitend binnen de beveiligde zakelijke cloudomgeving te werken, waardoor data niet lokaal op het privétoestel wordt opgeslagen.

Vraag 5:

Wordt er conform de AVG met regelmaat een Data Protection Impact Assessment (DPIA) uitgevoerd op de meest kritieke processen? Zo ja, wat is de datum van de meest recent uitgevoerde DPIA en op welke processen had deze betrekking?

Antwoord 5:

Ja, het uitvoeren van DPIA's is een vast onderdeel van ons privacybeleid bij processen met een hoog risico. Dit helpt ons om kwetsbaarheden in beeld te brengen voordat we nieuwe systemen of werkwijzen implementeren.

De meest recente DPIA is afgerond in november 2025 de DPIA voor de Collectieve Horeca Ontzegging beoordeeld. Hoewel de gemeente hierin een regierol vervult en niet de primaire verwerkingsverantwoordelijke is, hebben we dit assessment uitgevoerd om de privacy van betrokkenen te waarborgen. Daarnaast is in juni 2025 een DPIA uitgevoerd voor de applicatie en het proces rondom de aanpak van ondermijning.

Vraag 6:

Zijn er uit recente DPIA's of audits (zoals de ENSIA-audit) aanbevelingen voortgekomen die nog opvolging behoeven? Zo ja, om welke verbeterpunten gaat dit en op welke wijze wordt de raad over de voortgang hiervan geïnformeerd? (Vertrouwelijkheid ten aanzien van dit punt in acht genomen)

Antwoord 6:

De uitkomsten van audits en DPIA's worden door de ambtelijke organisatie opgepakt. Recente aanbevelingen hebben onder andere geleid tot een verscherping van het autorisatiebeheer (wie heeft toegang tot welke data?) en de verdere implementatie van het vier-ogen-principe bij kritieke processen.

Informatiebeveiliging is echter een continu proces; verbeterpunten worden structureel gemonitord. Uw raad wordt over de hoofdlijnen en de voortgang van deze verbeteringen jaarlijks geïnformeerd via de ENSIA-rapportage en de paragraaf bedrijfsvoering in de jaarstukken. Specifieke technische bevindingen blijven vanwege het veiligheidsrisico vertrouwelijk, maar zijn in te zien door de auditcommissie.

Vraag 7:

Is het college van mening dat er momenteel voldoende financiële middelen en expertise beschikbaar zijn om de data van onze inwoners veilig te houden? Zo nee, welke aanvullende middelen of maatregelen zijn volgens het college noodzakelijk?

Antwoord 7:

De gemeente Harderwijk beschikt over een solide basis en de nodige expertise om de huidige dreigingen het hoofd te bieden. Echter, de snelle technologische ontwikkelingen en de komst van de nieuwe Cyberbeveiligingswet (Cbw) leggen de lat steeds hoger.

Om aan deze strengere wettelijke eisen te blijven voldoen en onze digitale weerbaarheid te garanderen, zal informatiebeveiliging structureel aandacht en investering vragen. Dit betreft zowel de technische infrastructuur als het op peil houden van specialistische kennis. In de komende begrotingscycli zullen wij uw raad informeren over de middelen die nodig zijn om Harderwijk ook in de toekomst een digitaal veilige gemeente te laten blijven.

Wij gaan ervan uit dat wij hiermee uw vragen hebben beantwoord. Mocht u toch nog vragen hebben, dan kunt u contact opnemen met mevrouw J.M. van Hoof van Domein Bedrijfsvoering, afdeling I&A via m.vanhoof@meerinzicht.nl of telefoonnummer 085 1108 218.

Met vriendelijke groet,
Burgemeester en wethouders van Harderwijk,

A handwritten signature in blue ink, appearing to read 'C. Klaassen', with a large, sweeping flourish underneath.

de heer C. Klaassen
loco-secretaris

A handwritten signature in blue ink, appearing to read 'J. Joon', with a large, sweeping flourish underneath.

de heer J. Joon
burgemeester