voorstel

Zwolle

Raadsbrief over artikel 45 vragen

Datum 12 mei 2026

Onderwerp	Beantwoording artikel 45 vragen van CDA over Bescherming persoonsgegevens Zwollenaren
Versienummer	1
Portefeuillehouder	Paul Guldemond

Bijlagen

- Art 45 vragen: CDA-Bescherming persoonsgegevens Zwollenaren

Ontwerp besluit

De raad wordt voorgesteld kennis te nemen van de beantwoording van de artikel 45 vragen over de bescherming persoonsgegevens Zwollenaren.

Datum 12 mei 2026

Inleiding
Door het CDA zijn vragen gesteld over de cyberaanval bij de gemeente Epe. Hieronder treft u de beantwoording van deze vragen.

Kernboodschap

Vraag 1: Is het college bekend met de berichtgeving over de cyberaanval bij de gemeente Epe? Is het college het met het CDA eens dat Zwollenaren erop moeten vertrouwen dat de bescherming van persoonsgegevens op orde is?
Antwoord: het college is bekend met de berichtgeving over de recente cyberaanval bij de gemeente Epe, waarbij onbevoegden toegang hebben gehad tot systemen en persoonsgegevens van inwoners zijn buitgemaakt. Het college is het met het CDA eens dat Zwollenaren erop moeten kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden beschermd. In het raadsvoorstel *Robuuste Informatievoorziening (juli 2025)* hebben we dit als volgt opgeschreven; “we willen dat inwoners ons kunnen vertrouwen met hun data”.

Vraag 2: Hoe beoordeelt het college de kans dat een vergelijkbaar incident zich in onze gemeente voordoet?
Antwoord: het college doet er alles aan om cyberincidenten te voorkomen. Dit uit zich onder meer in training en opleiding, uitwijkprocedures en de implementatie van de cyberbeveiligingswet. Tegelijk onderkent het college dat absolute veiligheid niet bestaat en dat cyberdreigingen zich blijven ontwikkelen. Dat betekent dat, ondanks alle getroffen maatregelen en voortdurende aandacht voor informatiebeveiliging, nooit volledig kan worden uitgesloten dat ook Zwolle op enig moment wordt getroffen door een cyberaanval.

Vraag 3: Beschikt onze gemeente over een actueel plan voor het omgaan met cyberincidenten en datalekken?
Antwoord: in het raadsvoorstel *Robuuste Informatievoorziening* is de ambitie uitgesproken om te komen tot een volgend volwassenheidsniveau op het gebied van informatiebeveiliging. Zoals ook te lezen in het rekenkameronderzoek “Zwolle dataveilig?” is er een inhaalslag gemaakt op het gebied van informatiebeveiligingsbeleid 2022-2026. Vanwege aangescherpte Europese wetgeving (NIS2, in Nederland vertaald in de cyberbeveiligingswet CBW) wordt dit nu geactualiseerd. Bij onze informatiebeveiliging trekken we samen op met onze partner, het shared service centre ONS. Voor de continuïteit van de dienstverlening beschikt ONS over een professionele en zorgvuldig ingerichte back-up en herstelvoorziening, ingericht volgens gangbare beveiligingsstandaarden. Deze voorzieningen zijn gericht op het voorkomen van dataverlies en het spoedig herstellen bij verstoringen. Ook is er binnen ONS een team van gespecialiseerde securitymedewerkers actief, zowel technisch als beleidsmatig, waaronder een Chief Information Security Officer, een Privacy Officer en een Functionaris Gegevensbescherming. Periodiek worden er door derde partijen penetratietesten en audits uitgevoerd. De ICT omgeving wordt 24x7 gemonitord en waar nodig worden maatregelen aangescherpt.

Vraag 4: Wordt binnen onze gemeente actief gestuurd op dataminimalisatie, waarbij alleen persoonsgegevens worden opgeslagen die strikt noodzakelijk zijn, zo ja hoe?
Antwoord: dataminimalisatie is een belangrijk uitgangspunt binnen de gemeentelijke omgang met persoonsgegevens. De gemeente Zwolle wenst niet meer persoonsgegevens dan noodzakelijk te

verwerken voor het beoogde doel en (her)beoordeelt dit risicogestuurd bij de inrichting van nieuwe of bestaande informatiesystemen.
Binnen bijvoorbeeld het dataplatform van de gemeente Zwolle wordt dit uitgangspunt concreet toegepast. Voor het dataplatform is een expliciete *Data Protection Impact Assessment* (DPIA) uitgevoerd en vastgesteld, waarin onder meer is beoordeeld welke persoonsgegevens noodzakelijk zijn, hoe deze worden verwerkt en welke maatregelen worden getroffen om privacyrisico's te beperken.

Vraag 5: Zijn de geldende bewaartermijnen voor persoonsgegevens in alle systemen op orde en wordt hier actief op gecontroleerd?
Antwoord: de controle op naleving van bewaartermijnen vindt plaats op meerdere niveaus. De primaire verantwoordelijkheid ligt bij de proceseigenaar. Daarnaast wordt via interne audits, DPIA-processen en toezicht op informatie- en privacybeleid beoordeeld of de randvoorwaarden voor juiste toepassing van bewaartermijnen aanwezig zijn. Toezichtskaders zoals de *Eenduidige Normatiek Single Information Audit* (ENSIA) en IT-audits richten zich daarbij vooral op de governance, procesinrichting en technische borging, en niet op individuele dossiers of bestanden.
Het college onderkent dat, gezien de omvang en complexiteit van de gemeentelijke informatievoorziening, dit een voortdurende opgave is. Daarom wordt blijvend gewerkt aan het versterken van de structurele borging en het verbeteren van inzicht en controle op bewaartermijnen binnen systemen en processen. In het raadsvoorstel *Robuuste Informatievoorziening* is hiertoe uitgelegd hoe de invoering van een kwaliteitsmanagementsysteem bijdraagt aan continue verbetering van deze bewaartermijnen.

Vraag 6: Worden in Zwolle kopieën van identiteitsbewijzen opgeslagen en zo ja, in welke gevallen is dit noodzakelijk?
Antwoord: Het college vindt het van groot belang dat kopieën van identiteitsbewijzen alleen worden verwerkt en opgeslagen wanneer dit noodzakelijk is, en dat dit gebeurt in daarvoor bestemde systemen en met passende beveiliging. Binnen processen waar dit aan de orde kan zijn, wordt vooraf beoordeeld of het gebruik van kopieën noodzakelijk is voor het doel, of er een geldige grondslag is en waar deze gegevens veilig kunnen worden opgeslagen. Deze beoordeling gebeurt via een DPIA of een korte voorafgaande toets. In een grote organisatie kennen we meerdere processen waarin met identiteitsgegevens wordt gewerkt. In het gepubliceerde verwerkingsregister is transparant vastgelegd in welke processen dit voorkomt, zoals binnen HR waar dergelijke gegevens worden gebruikt voor werving en selectie en waar hiervoor geëigende procedures in het HR systeem zijn ingericht. Het college zet erop in dat waar kopieën van identiteitsdocumenten noodzakelijk zijn, deze zoveel mogelijk worden gecentraliseerd in het daarvoor bedoelde dossier of zaaksysteem. Door periodieke audits en de jaarlijkse actualisatie van het verwerkingsregister, in samenwerking met de afdelingen, houden we deze processen goed in beeld en worden ze waar nodig verder aangescherpt.

Vraag 7: Kan het college aangeven of er momenteel sprake is van verouderde systemen die een verhoogd risico vormen voor datalekken?
Antwoord: Het college onderkent dat binnen een grote en complexe informatievoorziening onderdelen kunnen voorkomen met verouderde techniek (legacy), die daarmee ook extra aandacht vragen vanuit informatiebeveiliging. Dit beeld wordt ook herkend in het rekenkameronderzoek "Zwolle dataveilig?", waarin wordt vermeld dat de accountant in de afgelopen jaren heeft gewezen op IT risico's en dat, ondanks gerealiseerde verbeterstappen, verdere stappen nodig blijven om tot kwalitatief goede

beheersing van IT risico’s te komen. Voortdurend worden kwetsbare applicaties vervangen of uitgefaseerd, als onderdeel van de reguliere levenscyclus van ons applicatielandschap.

Vraag 8: Op welke wijze wordt binnen de gemeentelijke organisatie aandacht besteed aan de menselijke factor in informatiebeveiliging, zoals bewustwording, training en het voorkomen van fouten door medewerkers, mede in het licht van eerdere incidenten bij onder andere Odido waarbij menselijke fouten een rol speelden?
Antwoord: Binnen de gemeente Zwolle worden medewerkers regelmatig getraind op het gebied van informatiebeveiliging en privacy volgens een jaarlijks bewustwordingsprogramma. Belangrijke onderdelen hiervan zijn meerdelige e-learningmodules (de gouden regels voor informatiebeveiliging), bestuurlijke bewustwording (onderdeel van de cyberbeveiligingswet) en een duidelijke plek in het onboardingsprogramma voor nieuwe medewerkers.

Openbaarheid
Deze nota is openbaar.

Burgemeester en wethouders van Zwolle,

burgemeester, Peter Snijders

secretaris, Dick Emmer