



Aan: College van Burgemeester en Wethouders

Onderwerp: Digitale veiligheid van persoonsgegevens inwoners gemeente Barneveld

Datum: 23-04-2026

Geacht college,

Op grond van artikel 41 van de organisatieverordening stelt de fractie van Pro'98 schriftelijke vragen over digitale veiligheid.

In een tijd waarin steeds meer van ons leven zich digitaal afspeelt, van belastingaangiften tot bezwaarschriften en van uitkeringsaanvragen tot identiteitsdocumenten, is de digitale infrastructuur van een gemeente minstens zo belangrijk als de fysieke. De gemeente is voor haar inwoners een vertrouwde hoeder: mensen zijn verplicht hun meest gevoelige gegevens aan te leveren. Naam, adres, geboortedatum, BSN. Het zijn niet zomaar data, het is iemands identiteit. Die verantwoordelijkheid is groot en vraagt om een zorgvuldige omgang.

Recentelijk werd bij de gemeente Epe, een Gelderse buurgemeente, pijnlijk zichtbaar hoe kwetsbaar gemeentelijke systemen kunnen zijn. Bij een cyberaanval werden persoonsgegevens van vrijwel alle ruim 32.000 inwoners gestolen. Namen, adressen, BSN-nummers, geboortedatum en bij meer dan duizend inwoners ook kopieën van identiteitsbewijzen kwamen in handen van criminelen. Gegevens waarmee iemand identiteitsfraude kan plegen, een bankrekening kan openen of een auto kan huren in het buitenland. De burgemeester van Epe sprak terecht niet van een lek, maar van diefstal: een ernstig misdrijf.

Helaas is de gemeente Epe geen uitzondering. Regelmatig verschijnen er berichten over datalekken bij gemeenten, zorginstellingen en bedrijven. De vraag is niet óf een cyberaanval kan plaatsvinden, maar of de gemeente voldoende voorbereid is wanneer dat gebeurt.

Pro'98 beschouwt de bescherming van persoonsgegevens van inwoners als een kernverantwoordelijkheid van de gemeente. Wij maken ons zorgen over de digitale weerbaarheid van Barneveld en stellen daarom de volgende vragen aan het college:

1. Is het college bekend met de cyberaanval op de gemeente Epe waarbij persoonsgegevens van vrijwel alle inwoners zijn gestolen? Heeft dit incident aanleiding gegeven tot intern overleg of aanvullende maatregelen?
2. Voldoet de gemeente Barneveld aantoonbaar aan de Baseline Informatiebeveiliging Overheid (BIO2) en de Cyberbeveiligingswet (CBW)?
 - a. Wanneer heeft de laatste externe audit of toetsing plaatsgevonden en wat waren de uitkomsten?
 - b. Hoe speelt de gemeente in op actuele ontwikkelingen en bedreigingen?

3. Hoe heeft de gemeente haar kritieke systemen beveiligd? Zijn er in het kader van recente ontwikkelingen (zoals bij gemeente Epe) verbeterpunten te identificeren binnen de huidige manier van werken?
 - a. Wordt er bij het opslaan van persoonsgegevens onderscheid gemaakt tussen tijdelijke bestanden/informatie, zoals inkomende documenten en aanvragen, en de centrale gemeentelijke systemen zoals de Basisregistratie Personen (BRP)?
 - b. Worden ontvangen documenten van inwoners, zoals bezwaarschriften en bijlagen met kopieën van identiteitsbewijzen, opgeslagen op aparte systemen? Zo ja, hoe zijn deze beveiligd en wie heeft daar toegang toe?
4. Hanteert de gemeente het principe van gegevensminimalisatie, en worden persoonsgegevens verwijderd zodra zij niet langer noodzakelijk zijn?
5. Worden gemeentelijke systemen actief gemonitord op verdachte activiteiten of ongebruikelijke toegangspatronen?
 - a. Houden we ontwikkelingen van datalekken in de gaten en passen we ons beleid waar nodig aan?
6. Zijn er de afgelopen twee jaar incidenten geweest waarbij ongeautoriseerde toegang tot gemeentelijke systemen of persoonsgegevens is vastgesteld of vermoed? Zo ja, hoe is daarmee omgegaan en is de raad daarover geïnformeerd?
7. Beschikt de gemeente over een actueel calamiteitenplan voor cyberincidenten, inclusief communicatie richting inwoners, melding bij de Autoriteit Persoonsgegevens en samenwerking met politie en het Nationaal Cyber Security Centrum?
8. Wordt er periodiek een cyberoefening uitgevoerd binnen de gemeente Barneveld of in regionaal verband? Zo nee, is het college bereid dit te organiseren?
9. Welke afspraken rondom datalekken en informatiebeveiliging zijn er gemaakt met externe leveranciers die gevoelige gegevens verwerken voor de gemeente?
10. Ontvangen medewerkers regelmatig en verplichte training op het gebied van digitale weerbaarheid, waaronder bewustwording rondom phishing en veilig wachtwoordgebruik?
11. Is er een interne meldcultuur waarbij medewerkers verdachte situaties over digitale weerbaarheid laagdrempelig kunnen melden?
12. Is het college bereid de raad voortaan jaarlijks te informeren over de staat van de digitale weerbaarheid binnen de gemeente, inclusief eventuele incidenten, audits en verbetermaatregelen, zodat de raad zijn controlerende rol op dit terrein adequaat kan vervullen?

Met vriendelijke groet,
Henri Mulder