gemeente Barneveld

Raadhuisplein 2
Postbus 63
3770 AB Barneveld
Telefoon 14 0342
Internet www.barneveld.nl
Whatsapp 0342495902

Datum:
6 juli 2026

Ons kenmerk:
-

Uw bericht van:
23 april 2026

Organisatieonderdeel:
Team I&A

Behandeld door:
V. Verhagen

Telefoonnummer:
-

Onderwerp:
Vragen over digitale veiligheid van persoonsgegevens inwoners gemeente Barneveld

Beste heer Mulder,

Op 23 april jl. heeft u namens uw fractie vragen gesteld over de digitale veiligheid van persoonsgegevens van inwoners van de gemeente Barneveld.
Met deze brief beantwoorden wij de gestelde vragen als volgt:

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?**
   Antwoord:
   Ja. Het college is bekend met het incident bij de gemeente Epe. Dit incident heeft geleid tot intern overleg en analyse. Het proces voor het installeren van security patches is aangescherpt naar aanleiding van deze analyse.

2. **Voldoet de gemeente Barneveld aantoonbaar aan de Baseline Informatiebeveiliging Overheid (BIO2) en de Cyberbeveiligingswet (CBW)?**
   Antwoord:
   Wij voldoen op dit moment nog niet volledig aan alle maatregelen uit de BIO2. Dit kwartaal starten wij met een gap-analyse, waarna een plan wordt opgesteld om ontbrekende maatregelen te implementeren.
   De Cyberbeveiligingswet (Cbw) is nog niet in werking getreden. De exacte invulling van de verplichtingen is nog in ontwikkeling. Wel voldoen wij in grote lijnen al aan de verwachte zorgplicht en meldplicht. Aan de registratieplicht wordt op dit moment gewerkt. Wij volgen de ontwikkelingen actief en treffen tijdig aanvullende maatregelen waar nodig.
   Overigens zal de BIO2 naar verwachting wettelijk verplicht worden onder de nieuwe Cyberbeveiligingswet.

   a. **Wanneer heeft de laatste externe audit of toetsing plaatsgevonden en wat waren de uitkomsten?**
      Antwoord:
      De gemeente legt jaarlijks verantwoording af via het ENSIA-proces. De verantwoording over 2025 wordt momenteel afgerond.
      De belangrijkste uitkomst is dat de gemeente op alle belangrijke punten voldoet aan de gestelde normen voor opzet en bestaan van maatregelen. Aandachtspunt is de vastlegging van controles. Hiervoor zijn verbeterafspraken gemaakt, die op korte termijn opnieuw worden getoetst.
      Daarnaast is begin 2026 door een externe auditor een audit op de Wet politiegegevens uitgevoerd. Deze audit laat een goed niveau van

compliance zien, met een vastgesteld verbeterplan richting de Autoriteit Persoonsgegevens.

b. **Hoe speelt de gemeente in op actuele ontwikkelingen en bedreigingen?**
Antwoord:
De gemeente volgt actief ontwikkelingen en dreigingen via onder andere het Nationaal Cyber Security Centrum, de Informatiebeveiligingsdienst voor gemeenten (IBD) en een extern Security Operations Center. Waar nodig worden maatregelen aangescherpt of geïmplementeerd.

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?**

Antwoord:
De gemeente beveiligt systemen op basis van risico-inschatting.
De beveiligingsorganisatie is ingericht met onder andere een Chief Information Security Office (CISO) en een Technical Information Security Officer (TISO), in samenwerking met de Privacy Officer en Functionaris Gegevensbescherming.
De belangrijkste systemen worden continu gemonitord door een extern Security Operations Center (SOC). Incidenten worden direct opgevolgd en maandelijks geanalyseerd om structurele verbeteringen door te voeren.
Jaarlijks worden penetratietesten uitgevoerd.
Ja, verbeterpunten zijn in beeld gebracht op basis van de periodieke analyse van incidenten, de resultaten van penetratietesten en de lessen die zijn getrokken uit externe incidenten, waaronder dat bij de gemeente Epe. Specifiek naar aanleiding van het incident bij de gemeente Epe is het patchproces voor kritieke systemen aangescherpt.

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)?**
Antwoord:
Ja. Er wordt onderscheid gemaakt tussen verschillende typen gegevens en systemen.
De Basisregistratie Personen wordt beheerd volgens de Wet BRP. Overige gegevens worden verwerkt binnen daarvoor ingerichte applicaties en processen.

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?**
Antwoord:
Ja. Ontvangen documenten worden opgeslagen in daarvoor bestemde applicaties volgens de daarvoor vastgelegde processen (bijvoorbeeld procedure Rechten van Betrokkenen, als het om persoonsgegevens gaat). De toegang tot deze applicaties is beperkt op basis van rol en autorisatie. De uitvoerenden zijn getraind en gehouden aan hun geheimhoudingsplicht.

4. **Hanteert de gemeente het principe van gegevensminimalisatie, en worden persoonsgegevens verwijderd zodra zij niet langer noodzakelijk zijn?**
   Antwoord:
   Ja. De gemeente hanteert het principe van gegevensminimalisatie en past dit toe bij de inrichting van processen, systemen en werkwijzen. Daarbij worden niet meer persoonsgegevens verwerkt dan noodzakelijk is voor het doel. Waar mogelijk worden gegevens geanonimiseerd of gepseudonimiseerd. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor het doel van de verwerking, tenzij een wettelijke bewaartermijn of andere wettelijke verplichting tot bewaring geldt. De gemeente richt haar processen, systemen en werkwijzen hierop in.

5. **Worden gemeentelijke systemen actief gemonitord op verdachte activiteiten of ongebruikelijke toegangspatronen?**
   Antwoord:
   Ja. Gemeentelijke systemen worden actief gemonitord op verdachte activiteiten door een extern Security Operations Center in samenwerking met eigen beheerders.

   a. **Houden we ontwikkelingen van datalekken in de gaten en passen we ons beleid waar nodig aan?**
      Antwoord:
      Ja. Ontwikkelingen rond datalekken worden actief gevolgd. Waar nodig worden beleid en maatregelen aangepast.

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?**
   Antwoord:
   Nee. Er zijn de afgelopen twee jaar geen incidenten vastgesteld of vermoed waarbij ongeautoriseerde toegang tot systemen of persoonsgegevens heeft plaatsgevonden. Wel worden regelmatig pogingen daartoe gedetecteerd. Deze zijn steeds tijdig gesignaleerd en tegengehouden.

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?**

   Antwoord:
   De gemeente ziet dat digitale weerbaarheid effect heeft op de samenleving en beschikt over een calamiteitenprotocol. In dit protocol staat beschreven op welke wijze wij optreden bij verschillende typen incidenten en calamiteiten. Het calamiteitenprotocol is generiek van aard en daarmee niet specifiek gericht op cyberincidenten. Bij een calamiteit wordt een zgn. calamiteitenoverleg ingericht. Het onderwerp communicatie maakt standaard onderdeel uit van dit overleg.
   Aanvullend geldt dat datalekken geregistreerd en, indien nodig, gemeld worden bij de Autoriteit Persoonsgegevens. Ook werken wij, voornamelijk via de Informatiebeveiligingsdienst voor gemeenten (IBD), samen met de politie, het Nationaal Cyber Security Centrum en andere landelijke partijen om

voorbereid te zijn op cyberincidenten.

8. **Wordt er periodiek een cyberoefening uitgevoerd binnen de gemeente Barneveld of in regionaal verband? Zo nee, is het college bereid dit te organiseren?**
   Antwoord:
   Op dit moment wordt er nog geen periodieke cyberoefening uitgevoerd binnen de gemeente Barneveld of in regionaal verband.
   Wel is er recent een tabletop-oefening gehouden en wordt op basis daarvan binnenkort een cyberoefening uitgevoerd. Dit sluit aan op de algemene crisis- en incidentenaanpak. Ook wordt gebruikgemaakt van de landelijke ondersteuning via de VNG/IBD, waaronder een cyberoefenpakket met oefenscenario's voor gemeenten.

9. **Welke afspraken rondom datalekken en informatiebeveiliging zijn er gemaakt met externe leveranciers die gevoelige gegevens verwerken voor de gemeente?**
   Antwoord:
   Afspraken met leveranciers worden gemaakt op basis van risico en wettelijke verplichtingen. Dit gebeurt onder andere via verwerkersovereenkomsten, GIBIT-voorwaarden en aanvullende eisen bij aanbestedingen.

10. **Ontvangen medewerkers regelmatig en verplicht training op het gebied van digitale weerbaarheid, waaronder bewustwording rondom phishing en veilig wachtwoordgebruik?**
    Antwoord:
    Ja. Nieuwe medewerkers worden tijdens hun introductieprogramma automatisch ingeschreven voor een door de CISO en Privacy Officer aangeboden training informatiebeveiliging en privacy.
    Daarnaast wordt momenteel een organisatiebrede aanpak geïmplementeerd waarbij medewerkers doorlopend worden getraind en bewust gemaakt van digitale risico's, zoals phishing en veilig wachtwoordgebruik. Deelname hieraan is, na instemming van de OR, verplicht gesteld.

11. **Is er een interne meldcultuur waarbij medewerkers verdachte situaties over digitale weerbaarheid laagdrempelig kunnen melden?**
    Antwoord:
    Ja. Medewerkers kunnen verdachte situaties over digitale weerbaarheid laagdrempelig melden, onder andere via de Servicedesk ICT en een meldknop in de e-mailomgeving voor verdachte e-mails. Vragen en signalen komen daarnaast regelmatig binnen bij de CISO, TISO en de Privacy Officer. Het belang van melden en bewustwording krijgt aandacht via de eerdergenoemde trainingen en via berichten op intranet.

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?**
    Antwoord:
    Ja. Het college is bereid de raad jaarlijks te informeren.

gemeente Barneveld

Met vriendelijke groet,
burgemeester en wethouders,

W. Wieringa	J. van der Tak
Secretaris	burgemeester