Nota voor Burgemeester en Wethouders

Team: Concernstaf
Onderwerp:
Vragen ex art. 46 RvO-D66-raadsmededeling datalek

Notagegevens		
Bestuursorgaan	:	B-en-W 11-02-2025
Notanummer	:	2025-90
Datum	:	11-02-2025
Programma	:	01 - Burger en bestuur
Portefeuillehouder	:	Burgemeester,Wethouder De Geest,
Bijlage(n)	:	Antwoordbrief vragen ex art 46 RvO-D66-datalek.docx,Schrijftelijke vragen data-lek.docx

Parafering

06-02-2025: Wethouder
06-02-2025: Burgemeester
10-02-2025: Programmamanager
08-02-2025: Chief information officer (CIO)

Agendering

* 07-02-2025: Teammanager Concernstaf en Adjunct-secretaris
* 07-02-2025: Gemeentesecretaris/algemeen directeur

Definitieve akkoord

11-02-2025

B & W d.d.: 11-02-2025

Besluit

1. De beantwoording van de vragen ex art 46 RvO van de D66-fractie vast te stellen
2. De beantwoording aan te bieden aan de raad

De nota en het besluit openbaar te maken

Inleiding

Per brief van 30 januari 2025 hebben A. de Bokx en O. Akdemir van de fractie van D66 uw college een aantal schriftelijke vragen ex art 46 RvO gesteld over raadsmededeling datalek. Bijgaand treft u de beantwoording aan.

Beoogd maatschappelijk resultaat

Kader

Betrokken partijen en participatie

Toelichting op participatiebeleid

1. Welke ruimte is er voor invloed? 2. Welke belangen hebben inwoners bij het project of de beleidsontwikkeling? 3. Hoeveel tijd, geld, capaciteit en expertise is beschikbaar? 4. College/raad stemt in met het voorgestelde participatieniveau (trede op de participatieladder) 5. Hoe verhoudt dit participatietraject zich tot andere lopende of toekomstige participatietrajecten?

Argumenten voor en tegen

Financiële consequenties en dekking

Openbaarmaking en communicatie

Aanpak en uitvoering

Gemeente Deventer
College van B&W Postbus 5000
7400 GC Deventer

Deventer, 30 januari 2025

Betreft: Schriftelijke vragen ex. Artikel 46 RvO
Onderwerp: Raadsmededeling data-lek

Geacht College,

Onze fractie waardeert dat de gemeente Deventer snel heeft opgetreden na het recente datalek en helder heeft gecommuniceerd over de genomen stappen. Transparantie en verantwoordelijkheid zijn essentieel in dergelijke situaties, en we erkennen de inzet van de betrokken medewerkers om dit incident zorgvuldig af te handelen.

Tegelijkertijd roept dit incident vragen op over de manier waarop gevoelige persoonsgegevens, waaronder BSN's en financiële gegevens, worden verwerkt en beveiligd. Het versturen van deze informatie via e-mail zonder extra waarborgen brengt risico's met zich mee en roept de vraag op of de huidige werkwijze voldoende voldoet aan de AVG en andere wet- en regelgeving.

Om herhaling in de toekomst te voorkomen en de bescherming van persoonsgegevens verder te versterken, willen wij enkele vragen stellen over de interne procedures, beveiligingsmaatregelen en naleving van de regelgeving:

1. Voldoet het verwerken en versturen van een bestand met BSN's en kredietgegevens via e-mail aan de AVG en andere relevante wetgeving?
2. Is er binnen de gemeente een expliciet beleid over het omgaan met gevoelige persoonsgegevens zoals BSN's en kredietgegevens?
3. Waarom is er gekozen om deze gegevens op deze manier te versturen, en was men zich bewust van de risico's?
4. Zijn er technische beperkingen binnen de gemeente die voorkomen dat gevoelige bestanden zonder beveiliging per e-mail worden verzonden?
5. Worden encryptie of andere beveiligingsmaatregelen standaard toegepast bij het delen van gevoelige persoonsgegevens? Zo niet, waarom niet?
6. Zijn medewerkers voldoende getraind in gegevensbescherming en bewust van de risico's van het werken met (bijzondere) persoonsgegevens?
7. Welke juridische risico's loopt de gemeente door deze manier van gegevensverwerking?
8. Overweegt het college een interne audit uit te voeren om te onderzoeken of er meerdere processen zijn waarbij grote hoeveelheden gevoelige gegevens op deze manier gedeeld worden?
9. Hoe wordt de gemeenteraad in de toekomst betrokken bij het verbeteren van de beveiliging van persoonsgegevens?

Alvast bedankt voor uw reactie.

Met vriendelijke groet,

Alex de Bokx & Oguzhan Akdemir

Grote Kerkhof 1
Postbus 5000
7400 GC Deventer

14 0570
telefoon

direct telefoonnummer

gemeente@deventer.nl
e-mail

Aan de fractie van D66
t.a.v.
A. de Bokx
O. Akdemir

Interne Post

2025-90 kenmerk		11 februari 2025 datum
M.C. Eggel contactpersoon	Schriftelijke vragen ex art 46 RvO onderwerp	

Geachte heer De Bokx en heer Akdemir,

In uw brief van 30 januari jl. hebt u ons college schriftelijke vragen ex art 46 RvO gesteld over de raadsmededeling Datalek. Ons antwoord is als volgt.

Vraag 1
Voldoet het verwerken en versturen van een bestand met BSN's en kredietgegevens via e-mail aan de AVG en andere relevante wetgeving?
Antwoord
Gezien de aard van de gegevens was e-mail in dit geval niet het geschikte middel om de gegevens te delen, daar zijn andere opties voor. De AVG vereist passende maatregelen bij het verwerken van persoonsgegevens. In dit geval was de intentie om de mail intern naar een collega te sturen en het datalek bewijst dat mailen foutgevoelig is.

Vraag 2
Is er binnen de gemeente een expliciet beleid over het omgaan met gevoelige persoonsgegevens zoals BSN's en kredietgegevens?
Antwoord
Ja, de gemeente heeft informatiebeveiligingsbeleid vastgesteld. Daarnaast worden medewerkers via structurele 'nanolearnings' gewezen op de risico's bij het werken met persoonsgegevens of anderszins vertrouwelijke informatie. Ook zijn er richtlijnen over het gebruik van Zivver (beveiligd mailen) opgesteld.

Vraag 3
Waarom is er gekozen om deze gegevens op deze manier te versturen, en was men zich bewust van de risico's?
Antwoord
De bedoeling was om de gegevens intern te versturen naar een collega. Als er (per ongeluk) een extern mailadres wordt ingevuld, dan geeft Zivver een waarschuwing dat er mogelijk gevoelige gegevens worden verstuurd. Ondanks deze melding is het in dit geval helaas toch misgegaan.

Vraag 4
Zijn er technische beperkingen binnen de gemeente die voorkomen dat gevoelige bestanden zonder beveiliging per e-mail worden verzonden?
Antwoord
Ja, medewerkers worden erop geattendeerd als zij op het punt staan mogelijk gevoelige bestanden te versturen.

Vraag 5
Worden encryptie of andere beveiligingsmaatregelen standaard toegepast bij het delen van gevoelige persoonsgegevens? Zo niet, waarom niet?
Antwoord
We hebben verschillende opties om persoonsgegevens, indien nodig, beveiligd te delen. Uitgangspunt is dat deze methoden worden gebruikt bij het delen van persoonsgegevens

Vraag 6
Zijn medewerkers voldoende getraind in gegevensbescherming en bewust van de risico's van het werken met (bijzondere) persoonsgegevens?
Antwoord
Medewerkers krijgen elke 3 weken lessen over informatiebeveiliging en privacy door middel van nanolearning. Naast deze lessen hebben we ook andere informatie/training en sessies.

Vraag 7
Welke juridische risico's loopt de gemeente door deze manier van gegevensverwerking?
Antwoord
De manier waarop de gegevensverwerking plaatsvond, is niet de werkwijze zoals die zou moeten zijn. Er zijn eerder immers al passende maatregelen genomen om risico's op datalekken zo klein mogelijk te maken. Desalniettemin is het recentelijk niet goed gegaan.

In het algemeen gesteld, kunnen gedupeerden van een datalek een schadeclaim indienen. Dit wordt alleen toegekend door de gemeente als kan worden aangetoond dat de indiener materiële of immateriële schade heeft geleden ten gevolge van het datalek.

Overigens achten wij het risico zeer klein dat er bij het recente datalek negatieve gevolgen optreden voor betrokkenen.

Vraag 8
Overweegt het college een interne audit uit te voeren om te onderzoeken of er meerdere processen zijn waarbij grote hoeveelheden gevoelige gegevens op deze manier gedeeld worden?
Antwoord
De gemeente was al vóór het datalek-incident bezig met het in kaart brengen van processen waarbij persoonsgegevens worden gebruikt. Hierbij worden ook risico's (waaronder risico's bij het versturen van gegevens) in kaart gebracht om passende maatregelen te kunnen nemen, waar nodig.

Vraag 9
Hoe wordt de gemeenteraad in de toekomst betrokken bij het verbeteren van de beveiliging van persoonsgegevens?
Antwoord
De gemeenteraad ontvangt jaarlijks een verslag opgesteld door de Chief Information Security Officer (CISO) en een verslag van de Functionaris Gegevensbescherming (FG), waarin ook aandacht zal worden besteed aan het verbeteren van de beveiliging van persoonsgegevens

Burgemeester en wethouders van de gemeente Deventer,
de secretaris, de burgemeester,

J.P. Wassens R.C. König