Nota voor Burgemeester en Wethouders

Team:
Onderwerp:
Toezichtjaarverslag 2024 van de Functionaris Gegevensbescherming (FG) en het jaarverslag 2024 van de Chief Information Security Officer (CISO).

Notagegevens		
Bestuursorgaan	:	B-en-W 18-03-2025
Notanummer	:	2025-179
Datum	:	18-03-2025
Programma	:	11 - Bedrijfsvoering
Portefeuillehouder	:	Burgemeester,
Bijlage(n)	:	Jaarverslag CISO 2024.pdf,Toezichtjaarverslag FG 2024.pdf

Parafering

13-03-2025: Burgemeester
13-03-2025: Chief information officer (CIO)

Agendering

* 13-03-2025: Gemeentesecretaris/algemeen directeur
* 14-03-2025: Teammanager Concernstaf en Adjunct-secretaris

Definitieve akkoord

18-03-2025

B & W d.d.: 18-03-2025

Besluit

1. Het toezichtjaarverslag van de Functionaris Gegevensbescherming over 2024 en het jaarverslag van de Chief Information Security Officer over 2024 vast te stellen.
2. De raadsmededeling vast te stellen en met het toezichtjaarverslag FG en jaarverslag CISO aan te bieden aan de gemeenteraad.

De nota en het besluit openbaar te maken

Inleiding

Toezichtjaarverslag FG 2024
De Functionaris Gegevensbescherming (FG) houdt binnen de gemeente toezicht op de toepassing en naleving van de privacywetgeving. Concreet gaat het om de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg). In het toezichtjaarverslag 2024 worden een aantal aandachtsgebieden behandeld. Per aandachtsgebied wordt beschreven in hoeverre de gemeente voldoende passende maatregelen heeft genomen en waar nodig worden aanbevelingen gedaan. Zo zijn de volgende positieve stappen te benoemen:
* Het verwerkingsregister is geactualiseerd, waardoor de gemeente beter inzicht heeft in welke structurele processen gebruik maken van persoonsgegevens.
* Om de bewustwording van medewerkers op peil te houden is ook in 2024 gebruik gemaakt van Nanolearnings.
* De intern gemelde datalekken zijn goed opgepakt en afgehandeld. Waar nodig is er op tijd melding gemaakt bij de Autoriteit Persoonsgegevens en zijn slachtoffers geïnformeerd.

Daarnaast worden er ook een aantal aanbevelingen gedaan, zoals:

* Actualiseer het privacybeleid van de gemeente, communiceer er intern over en maak het voor iedereen makkelijk vindbaar.
* Maak proceseigenaarschap minder vrijblijvend door te borgen dat management passende training krijgt over privacy.
* Er is een achterstand in het uitvoeren van DPIA's (privacy risicoanalyses). Gebruik het verwerkingsregister om een overzicht te maken van de processen waarop nog een DPIA moet worden uitgevoerd. Maak een prioritering in afstemming met de proceseigenaren.

Jaarverslag CISO 2024

De Chief Information Security Officer (CISO) rapporteert in zijn jaarverslag over de voortgang op het gebied van informatiebeveiliging binnen de gemeente. Het biedt een overzicht van de belangrijkste ontwikkelingen, risico's en verbetermaatregelen op het gebied van informatiebeveiliging, waarmee de gemeente haar weerbaarheid tegen cyberdreigingen verder versterkt.

Het verslag belicht diverse verbeteringen, zoals versterkte technische beveiligingsmaatregelen, bewustwordingscampagnes en het oefenen van het cybercrisisplan. Er blijven ook uitdagingen, zoals de complexiteit van het IT-landschap en de menselijke factor. Het blijft noodzakelijk om oude systemen uit te faseren, regelmatig risicoanalyses uit te voeren en medewerkers scherp te houden op de risico's van cyberdreigingen. Er is ook behoefte aan betere communicatie en eigenaarschap binnen de organisatie om informatiebeveiliging vanaf het begin in alle projecten en processen te integreren. Risicomanagement blijft een essentieel aandachtspunt, waarbij samenwerking tussen interne teams en externe partners/leveranciers cruciaal is.

Beoogd maatschappelijk resultaat
Gelet op de aard en omvang van de gegevensverwerking bij de gemeente Deventer is het van groot belang dat dit zorgvuldig gebeurt. De beginselen van de AVG, de Wpg en de BIO moeten daarbij in acht worden genomen.

Kader
Algemene Verordening Gegevensbescherming (AVG)
Wet Politiegegevens (Wpg)
Baseline Informatiebeveiliging Overheid (BIO)

Betrokken partijen en participatie

Toelichting op participatiebeleid
Niet van toepassing.

Argumenten voor en tegen
Voor
Voldoen aan verplichtingen uit de AVG, Wpg en de BIO.

Financiële consequenties en dekking
Niet van toepassing.

Openbaarmaking en communicatie
Het toezichtjaarverslag FG en jaarverslag CISO worden openbaar gemaakt.

Aanpak en uitvoering
Na het vaststellen van de nota worden de stukken aangeboden aan de gemeenteraad.
De directie stelt een plan op met daarin de verbeteracties voor privacy en informatiebeveiliging voor 2025.

RAADSMEDEDELING

Onderwerp	Toezichtjaarverslag 2024 van de Functionaris Gegevensbescherming (FG) en het jaarverslag 2024 van de Chief Information Security Officer (CISO).		
Nummer	2025-179	**Portefeuillehouder**	Burgemeester,
Team	DEV-CIO	**Datum**	18-03-2025

Inleiding
Het college informeert uw raad over het toezichtjaarverslag van de Functionaris Gegevensbescherming (FG) over 2024 en het jaarverslag van de Chief Information Security Officer (CISO) over 2024. De FG en de CISO van de gemeente Deventer zien erop toe dat de gemeente bij het verwerken van informatie en persoonsgegevens voldoet aan de verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG), de Wet Politiegegevens (Wpg) en de Baseline Informatiebeveiliging Overheid (BIO). De FG en CISO rapporteren hun bevindingen rechtstreeks aan het college van burgemeester en wethouders.

Kader
Algemene Verordening Gegevensbescherming (AVG)
Wet Politiegegevens (Wpg)
Baseline Informatiebeveiliging Overheid (BIO)

Kern van de boodschap
In 2024 heeft de gemeente weer de nodige verbetermaatregelen doorgevoerd op het gebied van privacy en informatiebeveiliging. Er wordt echter nog niet volledig aan aan de AVG, Wpg en BIO voldaan. Het uitvoeren van verplichte risicoanalyses en het borgen van proceseigenaarschap bij het management is een belangrijk punt van aandacht.

Nadere toelichting

Toezichtjaarverslag FG 2024
De Functionaris Gegevensbescherming (FG) houdt binnen de gemeente toezicht op de toepassing en naleving van de privacywetgeving. Concreet gaat het om de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg). In het toezichtjaarverslag 2024 worden een aantal aandachtsgebieden behandeld. Per aandachtsgebied wordt beschreven in hoeverre de gemeente voldoende passende maatregelen heeft genomen en waar nodig worden aanbevelingen gedaan. Zo zijn de volgende positieve stappen te benoemen:

* Het verwerkingsregister is geactualiseerd, waardoor de gemeente beter inzicht heeft in welke structurele processen gebruik maken van persoonsgegevens.
* Om de bewustwording van medewerkers op peil te houden is ook in 2024 gebruik gemaakt van Nanolearnings.
* De intern gemelde datalekken zijn goed opgepakt en afgehandeld. Waar nodig is er op tijd melding gemaakt bij de Autoriteit Persoonsgegevens en zijn slachtoffers geïnformeerd.

Daarnaast worden er ook een aantal aanbevelingen gedaan, zoals:

* Actualiseer het privacybeleid van de gemeente, communiceer er intern over en maak het voor iedereen makkelijk vindbaar.
* Maak proceseigenaarschap minder vrijblijvend door te borgen dat management passende training krijgt over privacy.
* Er is een achterstand in het uitvoeren van DPIA's (privacy risicoanalyses). Gebruik het verwerkingsregister om een overzicht te maken van de processen waarop nog een DPIA moet worden uitgevoerd. Maak een prioritering in afstemming met de proceseigenaren.

Jaarverslag CISO 2024
De Chief Information Security Officer (CISO) rapporteert in zijn jaarverslag over de voortgang op het gebied van informatiebeveiliging binnen de gemeente. Het biedt een overzicht van de belangrijkste

ontwikkelingen, risico’s en verbetermaatregelen op het gebied van informatiebeveiliging, waarmee de gemeente haar weerbaarheid tegen cyberdreigingen verder versterkt.

Het verslag belicht diverse verbeteringen, zoals versterkte technische beveiligingsmaatregelen, bewustwordingscampagnes en het oefenen van het cybercrisisplan. Er blijven ook uitdagingen, zoals de complexiteit van het IT-landschap en de menselijke factor. Het blijft noodzakelijk om oude systemen uit te faseren, regelmatig risicoanalyses uit te voeren en medewerkers scherp te houden op de risico's van cyberdreigingen. Er is ook behoefte aan betere communicatie en eigenaarschap binnen de organisatie om informatiebeveiliging vanaf het begin in alle projecten en processen te integreren. Risicomanagement blijft een essentieel aandachtspunt, waarbij samenwerking tussen interne teams en externe partners/leveranciers cruciaal is.

Het Toezichtjaarverslag FG 2024 en het Jaarverslag CISO 2024 zijn als bijlage bij deze raadsmededeling gevoegd. De directie stelt een plan op met daarin de verbeteracties voor privacy en informatiebeveiliging voor 2025.

Toezichtjaarverslag Functionaris Gegevensbescherming 2024

Gemeenten Deventer, Olst-Wijhe en Raalte

Opgesteld door: Lucas Klekamp

Inhoud

Managementsamenvatting 3
1. Inleiding 4
2. Governance 5
3. Verwerkingsregister 5
4. DPIA's 6
5. Privacyrechten 7
6. Training en bewustwording 8
7. Datalekken 8
8. Wet Politiegegevens 9

Managementsamenvatting

Dit verslag behandelt de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) door de gemeenten Deventer, Olst-Wijhe en Raalte in 2024. Het verslag is opgesteld door de Functionaris Gegevensbescherming (FG), de interne toezichthouder. Per aandachtsgebied wordt aangegeven in hoeverre voldoende maatregelen zijn genomen en welke aanbevelingen worden gedaan.

Governance
Het privacybeleid van de drie gemeenten is sinds 2018 niet meer geactualiseerd. Aanbevolen wordt om het beleid te actualiseren en daaruit voortvloeiende procedures definitief vast te stellen.
Er is een gebrek aan kennis en borging van proceseigenaarschap bij managers. Aanbevolen wordt om passende training te bieden en privacy onderwerpen op te nemen in onboardingstrajecten.

Verwerkingsregister
De verwerkingsregisters zijn in 2024 geactualiseerd en overgezet naar een SharePoint-omgeving. Zorg dat de registers ook actueel blijven door dit met een duidelijke procedure te borgen.

DPIA's
Er is een aanzienlijke achterstand in het uitvoeren van DPIA's (privacy risicoanalyses), waardoor mogelijke privacyrisico's niet in beeld zijn. Aanbevolen wordt om een overzicht te maken van de processen waarop nog een DPIA moet worden uitgevoerd en prioriteiten te stellen.

Privacyrechten
Inwoners worden nog onvoldoende over het gebruik van hun persoonsgegevens geïnformeerd. Dit kan verbeterd worden door op de website specifieke privacyverklaringen op te nemen.
Het aantal AVG-verzoeken (zoals verzoeken om inzage) is in 2024 in Deventer en Raalte aanzienlijk toegenomen. Aanbevolen wordt om de procedure voor het afhandelen van deze verzoeken te stroomlijnen door een procesbeschrijving vast te stellen en vindbaar te maken voor alle medewerkers.

Training en bewustwording
Medewerkers ontvangen elke 3 weken per e-mail Nanolearning lessen over privacy en informatiebeveiliging. Ongeveer 40% van alle medewerkers volgt deze lessen. Probeer (via management) om de deelname te verhogen. Daarnaast wordt aanbevolen om een verplichte onboardingstraining op te zetten voor nieuwe medewerkers over verantwoord omgaan met informatie.

Datalekken
In 2024 zijn de intern gemelde datalekken goed opgepakt en afgehandeld. Waar nodig is er melding gemaakt bij de AP en zijn slachtoffers geïnformeerd. Het aantal datalekken is in lijn met voorgaande jaren. Een grote meerderheid van de incidenten betreft het versturen van een brief of e-mail met persoonsgegevens naar de verkeerde ontvanger. Aanbevolen wordt om de geactualiseerde datalekkenprocedure vast te laten stellen door de directies.

Wet politiegegevens
Er zijn stappen gezet voor de implementatie van de Wet politiegegevens, maar er is nog veel werk te verzetten om volledig te voldoen. Aanbevolen wordt om prioriteit te geven aan het uitvoeren van DPIA's op boa-processen (toezicht & handhaving, sociale recherche en leerplicht).

1. Inleiding

Voor u ligt het toezichtjaarverslag van de Functionaris Gegevensbescherming (FG) over het jaar 2024. De FG houdt binnen een organisatie toezicht op de toepassing en naleving van de privacywetgeving. Concreet gaat het om de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) door de gemeenten Deventer, Olst-Wijhe en Raalte. Dit verslag is dan ook van toepassing op alle drie de DOWR-gemeenten. De verschillende bestuursorganen (college, burgemeester en gemeenteraad) zijn ieder voor zich eindverantwoordelijk voor het naleven van de AVG bij het uitvoeren van ieders gemeentelijke taken. Ten behoeve van de leesbaarheid van dit verslag wordt verder alleen 'de gemeente' gebruikt, in plaats van het steeds specifiek benoemen van een bestuursorgaan.

Per september 2024 heeft de vorige FG een andere functie aangenomen binnen de gemeente Deventer. Per 1 oktober 2024 heeft de huidige FG en opsteller van dit verslag haar opgevolgd.

Privacyregels zijn van toepassing op het gebruik van persoonsgegevens: oftewel, informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Voor de hand liggende persoonsgegevens zijn iemands naam, adres, telefoonnummer, BSN of pasfoto. Maar persoonsgegevens zijn bijvoorbeeld ook klant- of personeelsnummers, informatie over iemands gezondheid, camerabeelden of geluidsopnames waarop iemand te herkennen is, informatie over iemands inkomen of een IP-adres.
De gemeente verzamelt en gebruikt veel (gevoelige) persoonsgegevens om haar taken uit te kunnen voeren. Het gaat dan voornamelijk om gegevens van inwoners, maar ook van personen buiten de gemeente. Ook verzamelt de gemeente persoonsgegevens van haar medewerkers vanuit haar werkgeversrol. Vaak zijn mensen verplicht om hun persoonsgegevens aan de gemeente te verstrekken. Daarom moet iedereen erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat. Van belang hierbij is dat de AVG vereist dat de gemeente ook kan aantonen dat het gebruik van persoonsgegevens voldoet aan belangrijkste uitgangspunten van de AVG. Ook moet de gemeente kunnen laten zien dat er passende technische en organisatorische maatregelen zijn genomen om persoonsgegevens te beveiligen.

Dit verslag bestaat verder uit het behandelen van een aantal aandachtsgebieden die voortvloeien uit de AVG. Per aandachtsgebied wordt beschreven in hoeverre de gemeente voldoende maatregelen heeft genomen. Daarnaast worden waar nodig aanbevelingen gedaan.

2. Governance

Met governance wordt bedoeld het organiseren van de bescherming van persoonsgegevens binnen de organisatie. Het gaat om het opzetten van regels, processen en verantwoordelijkheden om ervoor te zorgen dat persoonsgegevens veilig en volgens de wet worden gebruikt. Het voldoen aan de AVG bij het gebruik van persoonsgegevens binnen de gemeentelijke processen is de verantwoordelijkheid van het lijnmanagement, de proceseigenaren[1]. De privacy officers ondersteunen hierbij en de FG houdt hier toezicht op. Het goed borgen van proceseigenaarschap is hierbij essentieel.
Dit begint bij het hebben van helder privacybeleid, waarin de taken en verantwoordelijkheden die voortvloeien uit de AVG in de organisatie worden belegd. In 2018 hebben de colleges van de drie gemeenten het Privacybeleidskader vastgesteld. Dit is echter sindsdien niet meer geactualiseerd. In een paar jaar tijd kan er behoorlijk veel veranderen op het gebied van privacy en binnen een gemeentelijke organisatie. Om ervoor te zorgen dat wat er op papier staat nog voldoende aansluit bij de werkelijkheid en vice versa, is het aan te raden het beleid periodiek te vernieuwen.
Daarnaast dient beleid waar nodig uitgewerkt te worden in procedures en richtlijnen voor het management en de rest van de medewerkers. In 2024 is een aantal procedures uitgewerkt en geactualiseerd door de privacy officers. Deze zijn echter nog niet definitief afgerond en vastgesteld door de directies van de drie gemeenten.

Goed proceseigenaarschap vereist meer dan alleen een papieren werkelijkheid in een beleidsdocument. Managers dienen voldoende kennis te hebben om hun verantwoordelijkheid daadwerkelijk te kunnen nemen. Dit betekent niet dat ze expert hoeven te zijn op het gebied van de AVG, maar ze moeten wel weten wat er van hen wordt verwacht, wat ze concreet moeten doen en wie ze daarbij kan ondersteunen. Op dit moment zijn er onvoldoende maatregelen genomen om dit te borgen. Privacy officers sluiten wel eens aan bij managementoverleggen om bepaalde onderwerpen toe te lichten, maar dit is ad hoc en te vrijblijvend. Opgedane kennis verdwijnt op het moment dat een manager vertrekt. De opvolger weet vervolgens niet wat er van hem/haar wordt verwacht.

<u>Aanbevelingen</u>

- Actualiseer het privacybeleid van de drie gemeenten, communiceer er intern over en maak het voor iedereen makkelijk vindbaar. Maak de in 2024 geactualiseerde procedures definitief en laat deze vaststellen door de drie directies. Zorg ook dat deze makkelijk vindbaar zijn.
- Maak proceseigenaarschap minder vrijblijvend. Zorg dat management passende training krijgt over privacy en maak het onderdeel van onboardingstrajecten, zodat ook nieuwe managers weten waar ze aan toe zijn en hun verantwoordelijkheid kunnen nemen. Het is aanbevolen om de onderwerpen informatiebeveiliging en informatiebeheer hierbij te betrekken.
  Voor gemeente Deventer specifiek geldt dat er momenteel een organisatieontwikkeling gaande is. Er gaat in 2025 volgens een nieuwe organisatiestructuur gewerkt worden waarbij sturende functies worden herzien. Gebruik dit als een kans om proceseigenaarschap beter te beleggen.

3. Verwerkingsregister

Op grond van de AVG en de Wpg zijn de gemeenten verplicht om een verwerkingsregister bij te houden. Dit register bestaat uit een overzicht van alle structurele processen binnen de gemeente waarbij persoonsgegevens worden gebruikt[2]. Per proces wordt aanvullende informatie opgenomen, zoals van wie persoonsgegevens worden gebruikt, om wat voor soort gegevens het gaat en hoe lang

[1] In Deventer de teammanagers, in Olst-Wijhe de teamleiders en in Raalte de domeinmanagers.
[2] In de AVG wordt de juridische term ‘verwerking’ gehanteerd. Dit betekent ‘elke handeling die je met persoonsgegevens kunt doen’.

ze worden bewaard. Naast dat het een verplichting is, is een actueel verwerkingsregister essentieel voor de gemeente om aantoonbaar aan de AVG te kunnen voldoen. Zie het als de kapstok voor de 'privacyboekhouding'. Het biedt inzicht in waar binnen de organisatie en op welke manier persoonsgegevens worden gebruikt. Zonder dit inzicht is het niet mogelijk om eventuele risico's te herkennen en passende maatregelen te nemen om persoonsgegevens te beschermen. Het dient als verwijsindex voor verdere documentatie, zoals DPIA's (privacy risicoanalyses), en het helpt de verantwoordelijkheden van proceseigenaren af te bakenen (wie is van welk proces).

In 2024 zijn goede stappen gezet ten aanzien van de drie verwerkingsregisters van de gemeenten. Er heeft weer een actualisatieslag plaatsgevonden. Dit was sinds 2018 niet meer gebeurd. Een privacy officer heeft hiervoor interviews afgenomen met medewerkers van (bijna) alle teams en domeinen en zo de benodigde informatie opgehaald. De registers zijn overgezet van Excelbestanden naar een SharePoint omgeving om het beheer ervan makkelijker te maken en de inhoud te kunnen delen met alle medewerkers in de organisatie. Veel geïnterviewde medewerkers gaven aan geïnteresseerd te zijn in wat er met hun input is gedaan en waar ze het register kunnen inzien. Het is van belang dat de registers ook bijgewerkt blijven en actiever gebruikt worden door proceseigenaren (met ondersteuning van privacy officers) om de naleving van de AVG aantoonbaar te maken. Om dit te borgen is een procesbeschrijving opgesteld, maar deze moet nog definitief gemaakt worden en door de directies vastgesteld worden.

<u>Aanbevelingen</u>

- Zorg voor een vastgestelde procedure om het verwerkingsregister actueel te houden. Neem proceseigenaren hierin mee, zodat zij weten wat hierbij hun verantwoordelijkheid is.
- Maak het register makkelijk vindbaar voor alle medewerkers en communiceer erover. Voorkom zo dat de registers weer in de 'digitale la' verdwijnen.
- Voor gemeente Deventer is het zaak om het verwerkingsregister aan te passen aan de nieuwe organisatiestructuur, zodra op de nieuwe manier gewerkt gaat worden.

4. DPIA's

Een Data Protection Impact Assessment (DPIA) is een risicoanalyse waarbij privacyrisico's in kaart worden gebracht binnen een werkproces. Zodat daarna passende maatregelen genomen kunnen worden om deze risico's te verkleinen. Het is verplicht om een DPIA uit te voeren op gemeentelijke processen met een hoog privacyrisico. Of er sprake is van zo'n hoog risico is aan de gemeente zelf om te beoordelen. Dit hangt bijvoorbeeld af van wat voor soort persoonsgegevens worden gebruikt (zoals gezondheidsgegevens), of er gebruikt wordt gemaakt van nieuwe technologie (zoals AI) of dat gegevens van kwetsbare personen worden gebruikt (zoals medewerkers of inwoners met hulpvragen). Voor een gemeente zijn veel processen 'DPIA-plichtig', omdat een gemeente nou eenmaal veel taken heeft waarbij zeer gevoelige persoonsgegevens verzameld moeten worden om die taken goed uit te voeren.

De DOWR-gemeenten hebben moeite om DPIA's uit te voeren op de processen waarbij dat verplicht is. Er is hierin een achterstand. Dit betekent dat mogelijke privacyrisico's niet in beeld zijn en dat de gemeente in veel gevallen onvoldoende kan aantonen dat een proces in lijn met de AVG wordt uitgevoerd. Bij mogelijke privacyrisico's valt te denken aan het verzamelen van te veel soorten persoonsgegevens, het onvoldoende informeren van inwoners over het gebruik van hun gegevens, het niet naleven van bewaartermijnen of het niet voldoende beveiligen van gegevens.
Voor het te weinig uitvoeren van DPIA's zijn een aantal oorzaken aan te wijzen. Zo is er geen compleet overzicht van de processen waarop nog een DPIA moet worden uitgevoerd, zodat ook niet helder is hoe groot de achterstand precies is. Dat maakt het lastig voor de directies om hierop te sturen en prioriteiten te stellen. Verder zijn proceseigenaren verantwoordelijk voor het uitvoeren van DPIA's op hun processen, maar weten vaak onvoldoende wat hierbij van hen wordt verwacht (zie

paragraaf 2). Ten slotte ondersteunen de privacy officers bij het uitvoeren van een DPIA. Dit team is echter, o.a. door personele wisselingen, niet op volledige sterkte geweest in 2024. Daarnaast ging veel van hun tijd naar andere taken, waaronder het coördineren van de vele AVG-verzoeken (zie paragraaf 5).

Aanbevelingen

- Gebruik de geactualiseerde verwerkingsregisters om een overzicht te maken van de processen waarop nog een DPIA moet worden uitgevoerd. Maak vervolgens een prioritering in afstemming met de proceseigenaren van de betreffende teams en domeinen.

5. Privacyrechten

De AVG geeft mensen verschillende rechten om controle te houden over hun persoonsgegevens. Zo hebben mensen het recht om te weten wat een organisatie met hun persoonsgegeven doet (het recht op informatie). En ze kunnen bijvoorbeeld vragen om inzage in hun gegevens of verzoeken om hun gegevens te laten wijzigen of verwijderen. Gehoor geven aan mensen die een beroep doen op hun privacyrechten draagt bij aan het vertrouwen in de gemeente. Het is van belang dat er voldoende maatregelen zijn genomen om op een juiste manier aan deze rechten te kunnen voldoen.

Om uitvoering te geven aan het recht op informatie hebben de gemeenten een privacyverklaring op hun website gepubliceerd. Deze verklaringen zijn echter te algemeen en daarom onvoldoende om aan de informatieverplichting te voldoen. Dit kan verbeterd worden door specifieke privacyverklaringen te publiceren op plekken op de website waar mensen wordt gevraagd om bepaalde persoonsgegevens te verstrekken. Bijvoorbeeld op de pagina die gaat over het aanvragen van een bijstandsuitkering. Of op plekken waar inwoners wordt gevraagd om bepaalde gegevens achter te laten via een webformulier.

Het aantal AVG-verzoeken (zoals verzoeken om inzage of verwijdering van persoonsgegevens) is in 2024 aanzienlijk toegenomen. DOWR-breed gaat het om 41 verzoeken ten opzichte van 18 verzoeken in 2023. Opmerkelijk is dat deze stijging alleen voor Deventer en Raalte geldt. In Olst-Wijhe komt er sporadisch een verzoek binnen. Dit kan ofwel betekenen dat er nauwelijks verzoeken worden gedaan. Of het betekent dat er wel verzoeken worden gedaan, maar dat deze binnen de teams niet altijd als zodanig worden herkend en geregistreerd.
De stijging van het aantal verzoeken leidt tot een aanzienlijke stijging in werkdruk voor de privacy officers die deze verzoeken coördineren, maar ook voor de betreffende teams en domeinen waar de verzoeken op zien. Omdat de reactie van de gemeente op een verzoek een besluit is (vergelijkbaar met een WOO-verzoek), heeft dit in sommige gevallen tot een bezwaarprocedure geleid. Dit brengt ook weer de nodige werkdruk met zich mee. Niet alle proceseigenaren weten voldoende dat ze een rol hebben in de afhandeling van dit soort verzoeken en vaak voelt het als werk dat ‘erbij’ komt. Terwijl het kunnen voldoen aan dit soort verzoeken onderdeel zou moeten zijn van de reguliere bedrijfsvoering. Dit leidt soms tot discussies over wie wat moet doen.
Om het afhandelingsproces te stroomlijnen en de verantwoordelijkheden duidelijker te beleggen hebben de privacy officers in 2024 gewerkt aan een nieuwe procesbeschrijving. Deze dient nog vastgesteld te worden door de directies.

Aanbevelingen

- Verbeter de informatie over het gebruik van persoonsgegevens door de gemeente door het publiceren van aanvullende privacyverklaringen op plekken op de website waar om persoonsgegevens wordt gevraagd (bijvoorbeeld bij webformulieren). Ook wordt aanbevolen om ter bevordering van de transparantie een versie van het verwerkingsregister te publiceren.

- Laat de nieuwe procesbeschrijving voor AVG-verzoeken vaststellen door de directies, maak het makkelijk vindbaar en communiceer er intern over.

6. Training en bewustwording

Om de bewustwording op peil te houden is ook in 2024 gebruik gemaakt van het Nanolearning programma. Hierbij krijgen alle medewerkers van de DOWR-gemeenten elke 3 weken per e-mail een korte les over privacy en informatieveiligheid. Gemiddeld worden deze lessen door 40% van alle medewerkers doorgenomen.
Omdat de lessen voor alle medewerkers te volgen moeten zijn, zijn deze vrij algemeen van aard. Sommige medewerkers hebben echter aanvullende privacytraining nodig, afhankelijk van welke taken medewerkers uitvoeren. Zo werken medewerkers in het sociaal domein met zeer gevoelige informatie en moeten zij regelmatig lastige afwegingen maken over wat ze wel of niet aan gegevens over iemand opvragen of opnemen in een dossier. Specifieke privacytraining voorkomt onnodig (onrechtmatig) gebruik van persoonsgegevens, maar ook eventuele handelingsverlegenheid bij medewerkers. Er is in 2024 wel een aantal presentaties gegeven door de privacy officers binnen bepaalde teams en domeinen. Hoewel uiteraard zeer belangrijk en nuttig, gebeurt dit nog ad hoc. Het borgen van voldoende structurele training ontbreekt nog.

<u>Aanbevelingen</u>

- Ga door met het aanbieden van de Nanolearning lessen. Probeer het deelnamepercentage te verhogen door medewerkers (via management) zo veel mogelijk intrinsiek te motiveren de lessen te volgen.
- Van medewerkers van een gemeente mag worden verwacht dat ze de nodige digitale vaardigheden hebben om hun werk verantwoord uit te kunnen voeren. Het is aanbevolen een verplichte onboardingstraining voor nieuwe medewerkers te ontwikkelen over verantwoord omgaan met informatie (waaronder persoonsgegevens). Doe dit in samenhang met andere disciplines als informatiebeveiliging en informatiebeheer.

7. Datalekken

Een datalek is een beveiligingsincident wat tot gevolg heeft dat persoonsgegevens onterecht of ongewenst worden ingezien, verstrekt, verloren, vernietigd of gewijzigd. Datalekken komen voor bij alle organisaties en zijn op zichzelf niet onrechtmatig. Wel moeten er passende maatregelen worden genomen om de kans op een datalek zo klein mogelijk te maken. En als het toch gebeurt moet er, afhankelijk van het risico op nadelige gevolgen, een melding worden gedaan bij de Autoriteit Persoonsgegevens (AP). Ook dienen slachtoffers in sommige gevallen geïnformeerd te worden over het datalek.

In 2024 zijn de intern gemelde datalekken goed opgepakt en afgehandeld. Waar nodig is er op tijd melding gemaakt bij de AP en zijn slachtoffers geïnformeerd. Het aantal datalekken is in lijn met voorgaande jaren. Een grote meerderheid van de incidenten betreft het versturen van een brief of e-mail met persoonsgegevens naar de verkeerde ontvanger. Waar nodig is er overleg geweest tussen de betreffende managers en een privacy officer en zijn er maatregelen genomen op de kans op datalekken te verkleinen.
De procedure voor de afhandeling van datalekken is in 2024 geactualiseerd, maar is nog niet vastgesteld door de directies.

<u>Aanbevelingen</u>

- Laat de geactualiseerde datalekkenprocedure vaststellen door directie en maak deze makkelijk vindbaar voor medewerkers.

8. Wet Politiegegevens

Wanneer een Buitengewoon Opsporingsambtenaar (boa) persoonsgegevens gebruikt in de rol van toezichthouder is de AVG van toepassing. Maar als gegevens worden gebruikt voor de opsporingstaak geldt een ander kader, namelijk de Wet Politiegegevens (Wpg). Voor gegevens die onder dit regime vallen gelden andere (strengere) regels. Bijvoorbeeld over bewaartermijnen en over wanneer gegevens gedeeld mogen worden met een derde. De Wpg is binnen gemeente Deventer van toepassing op team Toezicht & Handhaving, de sociale recherche en leerplichtambtenaren. Voor Olst-Wijhe en Raalte gaat het alleen om de leerplichtambtenaren.[3]

In 2024 zijn stappen gezet ten behoeve van de implementatie van de Wpg. Zo zijn de Wpg processen toegevoegd aan de verwerkingsregisters en is de FG (naast AVG toezichthouder) ook aangewezen als Wpg toezichthouder. Binnen team Toezicht & Handhaving in Deventer zijn ook een aantal verbetermaatregelen genomen. Ook is de verplichte interne privacy audit (zelfevaluatie) weer uitgevoerd.
Uit de audit kwam naar voren dat er echter nog veel werk te verzetten is om volledig aan de Wpg te voldoen. In 2025 wordt er een externe privacy audit uitgevoerd over het jaar 2024. De resultaten daarvan worden gedeeld met de AP.

<u>Aanbevelingen</u>

- Neem de nodige maatregelen om aan de Wpg te voldoen. Geef prioriteit aan het uitvoeren van DPIA's op de boa processen waarin politiegegevens worden gebruikt.

[3] Team Toezicht & Handhaving en team Inkomensondersteuning (sociale recherche) in Deventer verwerken ook politiegegevens die betrekking hebben op inwoners uit Olst-Wijhe en Raalte. Gemeente Deventer is als werkgever van de betreffende boa's verantwoordelijk voor het voldoen aan de Wpg.

Rapportage 2024

Informatiebeveiliging

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

CISO | Februari 2025

1. Inleiding

In 2024 hebben de DOWR-gemeenten belangrijke stappen gezet op het gebied van informatiebeveiliging. Zo zijn er aanzienlijke verbeteringen doorgevoerd op het vlak van technische informatiebeveiliging, zijn er meerdere bewustwordingscampagnes georganiseerd en hebben we het cybercrisisplan geoefend.

De toenemende digitalisering van gemeentelijke diensten, gecombineerd met een stijgend aantal cyberdreigingen, benadrukt het belang van een sterke beveiligingsstrategie. Dit jaarverslag biedt een overzicht van de belangrijkste ontwikkelingen, risico's en verbetermaatregelen.

1.1. Successen

Betrokkenheid van medewerkers: Steeds meer collega's melden verdachte situaties en we hebben een actief en vast aantal deelnemers dat aan onze bewustwordingstrainingen (Nanolearning) deelneemt. Dit toont aan dat informatiebeveiliging binnen de organisaties leeft. Ook de IT-teams tonen steeds meer pro-activiteit in het verbeteren van de beveiligingsmaatregelen, wat essentieel is voor het minimaliseren van risico's.

1.2. Uitdagingen

Complexiteit van informatiesystemen: De variëteit aan IT-systemen, van verouderd tot modern, vraagt om risicomanagement, regelmatige updates en uitfasering van oude systemen.

Menselijke factor: Ondanks vooruitgang in bewustwording blijft de menselijke factor een kwetsbare schakel in onze beveiligingsstrategie. Fouten en onzorgvuldigheid brengen risico's met zich mee. Het is een doorlopend proces om medewerkers alert te houden en hen de juiste middelen en kennis te bieden voor een effectieve omgang met cyberdreigingen.

Proceseigenaarschap & vindbaarheid: Medewerkers raken steeds meer betrokken bij informatieveiligheid, maar er is vaak onduidelijkheid over proceseigenaarschap en de verantwoordelijkheden voor beveiliging. Het informatieveiligheidsteam wordt niet altijd tijdig betrokken bij nieuwe initiatieven. Dit benadrukt de noodzaak van betere communicatie en vindbaarheid, zodat informatieveiligheid vanaf het begin in alle projecten wordt geïntegreerd.

Risicomanagement: We hebben belangrijke stappen gezet, maar risicomanagement moet verder in de organisatie worden ingebed. De veranderende cyberdreigingen vereisen een dynamische aanpak en nauwe samenwerking tussen interne teams en externe partners.

2. Weerbaarheid

In 2024 zagen we een toename in het aantal cyberrisico's die een reële dreiging vormden voor de DOWR-gemeenten. Deze risico's bedreigen niet alleen onze systemen, maar ook de dienstverlening aan burgers. Enkele van deze risico's zijn:

- Datalekken: Bijvoorbeeld door phishing of menselijke fouten.
- Verstoringen: Dreigingen gericht op systemen van dienstverleners of partners, zoals DigiD.
- Afhankelijkheid van leveranciers: Beveiligingsproblemen bij externe partijen hebben ook impact op ons.

Om deze risico's te beheersen, hebben we onze processen aangescherpt en aanvullende maatregelen geïmplementeerd om de weerbaarheid van organisaties te verhogen.

2.1. Schaduw-IT incident

In 2024 werd in Deventer een beveiligingsincident vastgesteld via een niet-zakelijke internetverbinding, veroorzaakt door een fout in de netwerkinstellingen. Dit systeem viel buiten het beheer en de infrastructuur van onze organisatie, maar werd wel door een leverancier gebruikt. Dankzij de snelle detectie en het directe ingrijpen van DOWR-i kon schade worden voorkomen. Dit benadrukt niet alleen het belang van effectieve detectie- en responsmechanismen, maar ook de noodzaak om het gebruik van niet-goedgekeurde IT-systemen, software of clouddiensten terug te dringen en systemen structureel te beheren.

2.2. Informatiebeveiligingsdienst meldingen

Als overheidsorganisatie ontvangen wij meldingen van de Informatiebeveiligingsdienst (IBD) over kwetsbaarheden in onze applicaties, apparatuur en diensten, die wij vervolgens verifiëren en verhelpen.

Het aantal gemelde kwetsbaarheden is aanzienlijk afgenomen, voornamelijk doordat we verouderde software hebben uitgefaseerd. We ontvangen ook

meldingen die, na controle door de specialisten, niet meer relevant zijn voor ons (n.v.t.).

Tabel 1: Afname gemelde kwetsbaarheden

Gemelde kwetsbaarheden	*2022*	*2023*	*2024*
Totaal aantal gemelde kwetsbaarheden	282	240	**134**
Kwetsbaarheden n.v.t.	76	59	**42**
Kwetsbaarheden doorgezet naar oplosgroep	206	181	**92**

3. Beveiligingsmaatregelen

In 2024 hebben we diverse acties genomen om onze informatiebeveiliging te versterken, waaronder:

3.1. Technische verbeteringen

Wij hebben veelal geplande beveiligingsupdates doorgevoerd, verouderde systemen uitgefaseerd en technische versterking toegepast om kwetsbaarheden te minimaliseren. Dit proces versterkt onze systemen door onnodige onderdelen te verwijderen, rechten te beperken en beveiligingsmaatregelen zoals (moderne) encryptie te implementeren.

De technische beveiliging van onze systemen voldoet volledig aan de Baseline Informatiebeveiliging Overheid (BIO) en de opmaat naar de nieuwe versie van de BIO (2.0).

Hoewel deze stappen essentieel zijn, blijft het belangrijk om ook onze applicaties goed in te richten, gebruikersrechten zorgvuldig te beheren en bewust om te gaan met de informatie in deze systemen.

3.2. Samenwerking regio

Ook hebben we extra aandacht besteed aan het verbeteren van samenwerking met omliggende gemeenten om informatie te delen en gezamenlijk op te treden tegen dreigingen. Dit speelt onder andere in de veiligheidsregio IJsselland, alsook politie Oost-Nederland.

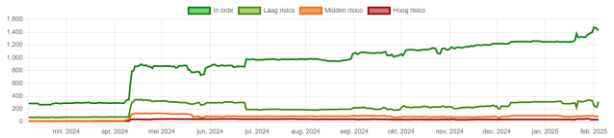
3.3 Compliance / ENSIA

Met ENSIA verantwoorden we ons gemeentebreed over informatieveiligheid. De kern is om de informatiebeveiliging op een hoog niveau te houden. Hiermee zorgen we ervoor dat de inwoners van onze gemeente erop kunnen vertrouwen dat hun gegevens in veilige handen zijn. Ook maakt dit ons een betrouwbare partner voor bedrijven en andere organisaties.

3.4. Naleving informatieveiligheidstandaarden

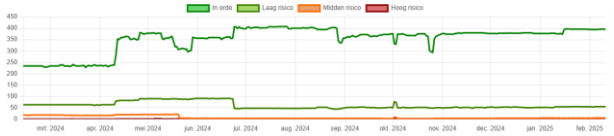
In 2024 zijn er stappen gezet met de webteams om meer beheersing te krijgen over de naleving van de informatiebeveiligingsstandaarden op onze websites. Dit heeft geleid tot een aanzienlijke vermindering van het aantal hoog-risico webdomeinen sinds begin 2024. Daarmee versterken we de digitale weerbaarheid van onze organisatie en komen we steeds beter in lijn met de geldende overheidsnormen voor informatieveiligheid van webdomeinen.

Afbeelding 2: Naleving informatiebeveiligingsstandaarden Deventer over 2024



Afbeelding 3: Naleving informatiebeveiligingsstandaarden Raalte over 2024

Afbeelding 4: Naleving informatiebeveiligingsstandaarden Olst-Wijhe over 2024



4. Bewustwording en training

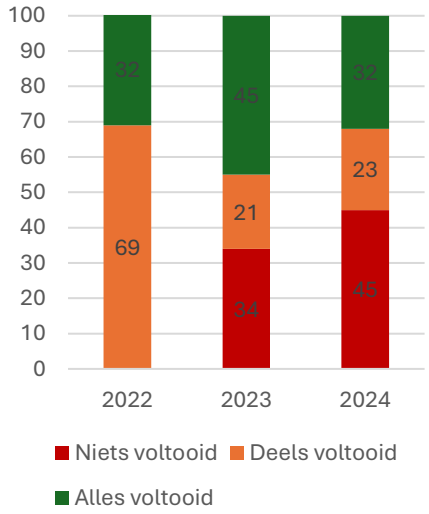
Een weerbare organisatie begint bij goed geïnformeerde en getrainde medewerkers. In 2024 hebben we:

- Cybercrisis oefening: We hebben eind 2024 een succesvolle cybercrisis oefening gehouden om ons crisisplan en de communicatielijnen te testen, met duidelijke leerpunten voor verbetering.

- Securityblog: We hebben een securityblog opgezet en zijn actiever op het intranet, wat onze zichtbaarheid en communicatie over cybersecurity vergroot.

- Bewustwordingscampagnes georganiseerd: Gerichte campagnes voor het herkennen van cyberdreigingen. Dit doen we onder andere door middel van korte lessen elke 3 weken per e-mail over Privacy en Informatiebeveiliging en intranetberichten met specifieke onderwerpen.
- Het gemiddelde percentage medewerkers dat deelnam aan de trainingen in 2024 ligt rond de 40%. Over het gehele jaar zien we echter dat het aantal medewerkers dat de lessen actief volgt terugloopt t.o.v. voorgaande jaren, zie figuur 1.

Figuur 1: Nanolearning deelname over 2022-2024 (%)



- Red Teaming oefening: Tijdens een Red Teaming oefening (waarbij onze beveiliging wordt getest door een 'tegenpartij') zijn er verbeterpunten geïdentificeerd in zowel de digitale als fysieke beveiliging. Ook werd duidelijk dat het bewustzijn van medewerkers verhoogd moet worden. Deze bevindingen worden meegenomen in onze acties.

5. Informatiebeveiligingsplan 2024

In lijn met het Informatiebeveiligingsplan 2024 zijn er belangrijke stappen gezet op het gebied van informatiebeveiliging binnen de gemeente. Echter, een aantal belangrijke onderdelen zoals de implementatie van risicomanagement, het beleid uitlijnen in de organisaties en dataclassificatie bevinden zich nog in uitvoering. Deze vertraging is deels het gevolg van de uitgestelde vaststelling van de Cyberbeveiligingswet en de afhankelijkheid van lopende organisatorische processen.

Onderwerp	Voortgang
Techniek	
Toepassen geoblocking	Afgerond
Meer functionaliteit op laptops	Afgerond
Pilot: sneller en beter reageren met Security AI	Afgerond
Zorgen voor een basisbeveiliging	Afgerond
Organisaties toetsen met ENSIA	Afgerond
Mens	
Vormgeven sturingsinformatie directie	Afgerond
Nanolearning lessen	Afgerond
Cybercrisis oefenen	Afgerond
Introductietraining medewerkers	In uitvoering
Organisatie	
Red Teaming	Afgerond
Beleid uitlijnen met organisaties	In uitvoering
Implementeren risicomanagement / ISMS	In uitvoering
Inzichtelijk maken impact NIS2 / ISO27001	In uitvoering
Implementeren Dataclassificatie	In uitvoering

6. Vooruitblik 2025

Voor 2025 zijn er een aantal strategische prioriteiten opgesteld in het jaarplan met als thema een ‘Digitaal verantwoord DOWR’:

- **Bewustzijn vergroten:** Zorgen dat iedereen in de organisatie begrijpt wat er nodig is om gegevens veilig en privacyvriendelijk te verwerken.
- **Eigenaarschap versterken:** Duidelijk toewijzen van verantwoordelijkheden binnen processen, zodat informatiebeveiliging en privacy niet alleen op papier geregeld zijn, maar ook daadwerkelijk worden toegepast.
- **Dataclassificatie toepassen:** Investeren in het juist classificeren van data, zodat gevoelige informatie op een passende manier wordt beschermd en verwerkt.
- **Risico’s beheersen:** Door Information Risk Management (IRM) systematisch toe te passen, kunnen risico’s tijdig worden geïdentificeerd en gemitigeerd.

7. Reflectie van de CISO

Informatiebeveiliging gaat niet alleen om het voorkomen van incidenten, maar ook om het bouwen van vertrouwen bij onze inwoners. Zij vertrouwen erop dat hun gegevens veilig zijn bij ons en dat wij altijd in staat zijn om onze diensten te leveren.

De inzet voor komend jaar is om samen met de organisaties informatiebeveiliging verder te integreren in ons dagelijkse werk. Het moet niet alleen een verantwoordelijkheid zijn van IT of de (C)ISO, maar een gedeelde verantwoordelijkheid van iedereen. Samen kunnen we een digitale omgeving creëren die veilig, betrouwbaar en toekomstbestendig is.