Jaarverslag 2024

Informatieveiligheid, gegevensbescherming en WPG

gemeente
NOORDOOSTPOLDER

Gemeente Noordoostpolder

DATUM

Inhoudsopgave

1. Inleiding

Onze inwoners, ondernemers en samenwerkingspartners moeten erop kunnen vertrouwen dat hun gegevens bij de gemeente veilig zijn en dat hun privacy gerespecteerd wordt. Dat betekent dat eisen gesteld worden aan de bescherming van deze gegevens in lijn met vigerende wetgeving zoals de (u)AVG, de WPG[1] en de Baseline informatiebeveiliging Overheid.

Meer concreet zijn de eisen, zoals opgenomen in het strategisch beleid informatieveiligheid en privacy van de gemeente:

- Gegevens moeten op orde en controleerbaar zijn
- Gegevens en informatie mogen alleen verwerkt worden als ze nodig zijn voor uitvoering van onze gemeentelijke taken
- Gegevens en informatie mogen alleen beschikbaar zijn voor de daartoe geautoriseerde personen
- Gegevens moeten voor hen beschikbaar zijn en mogen niet onderschept, gelezen of gemanipuleerd kunnen worden
- Medewerkers moeten zorgvuldig en bewust handelen om bovenstaande te borgen.
- Doelstellingen en beginselen uit de AVG moeten we waarborgen
- Onze toezichthouders moeten voldoen aan de Wet politiegegevens

Dit jaarverslag gaat in op de informatieveiligheid (hoofdstuk 2), een verslag over de AVG (hoofdstuk 3) en de bevindingen over de WPG (hoofdstuk 4).

[1] Algemene Verordening Gegevensbescherming en Wet Politiegegevens

2. Informatieveiligheid

Geldende kaders informatieveiligheid

- Voor gemeenten is de Baseline Informatiebeveiliging Overheid (BIO) als standaard voor de informatiebeveiliging binnen de Nederlandse overheid een belangrijk verplicht kader. De BIO bevat regels en richtlijnen die zijn ontworpen om ervoor te zorgen dat de gemeente hun informatie veilig beheert. Deze maatregelen helpen om de gemeente te beschermen tegen cyberaanvallen, datalekken en andere beveiligingsrisico's.
- De 10 principes voor informatiebeveiliging van de VNG zijn een bestuurlijke aanvulling hierop. Hierin wordt ingegaan op de verantwoordelijkheid van bestuurders voor de informatiebeveiliging binnen gemeentelijke organisatie.

Grootste risico's informatieveiligheid

Cybercriminaliteit neemt de afgelopen jaren drastisch toe in zowel frequentie als complexiteit, met een groeiende impact. Meest voorkomende vormen zijn:

1		Malware in de vorm van virussen, cryptolockers en spyware.
2		Aanvallen op de ICT infrastructuur en de webapplicaties door hackers. Zeker door de toename van nation state hacks is dit een grote bedreiging.
3		Spam en Phishingmails worden in grote hoeveelheid verspreid.

Het goed inrichten van informatiebeveiliging in de breedste zin van het woord voorkomt extra tijdsinvestering en herstelkosten achteraf. De uitdaging is om te zorgen dat informatie op het juiste moment beschikbaar is, voor onze medewerkers, inwoners, ondernemers en samenwerkingspartners. Ook nadat zaken afgehandeld zijn. Iedereen moet erop kunnen vertrouwen en dat hun data juist en volledig is èn dat dit niet door kwaadwillende kan worden onderschept (weerbaarheid).

Informatiebeveiligingsdienst gemeenten (IBD)

Gemeenten worden ondersteund bij het treffen van beveiligingsmaatregelen en bij het versterken van hun digitale weerbaarheid door een aparte dienst van de VNG. De IBD biedt veel voorbeeldproducten waar gemeenten mee kunnen werken aan hun informatieveiligheid. Ze focussen zich tegenwoordig meer op cyberweerbaarheid en het ontwikkelen van producten die voldoen aan de nieuwste wetgeving op gebied van informatieveiligheid en AI. Hun informatie en voorbeelden worden binnen de gemeente gebruikt als basis voor de beveiligingsmaatregelen.

De gemeente heeft in 2024 een geactualiseerde ICT-foto aan de IBD verstrekt. Op basis van deze foto ontvangt de gemeente meer gericht kwetsbaarheidsmeldingen. ICTbeheer screent deze meldingen en treft waar nodig maatregelen. We zien (gelukkig) vaak dat dit kwetsbaarheden betreft waarvoor de leveranciers al updates hebben. Deze updates zijn meestal al bekend en doorgevoerd of al gepland. We ontvingen daarnaast berichten over

actuele dreigingen, zoals phishingcampagnes met adviezen hoe te voorkomen dat de omgeving van Gemeente Noordoostpolder vatbaar is voor genoemde typen aanvallen. In voorkomende gevallen zijn de geadviseerde maatregelen doorgevoerd.

In 2024 is op onze website een zogenoemde Coördinated Vulnerability Disclosure geplaatst met een meldformulier. Hiermee geeft de gemeente aan dat ze open staat voor meldingen van kwetsbaarheden van buitenaf. Zo kunnen externen kwetsbaarheden melden en zien ze de spelregels die de gemeente hierbij hanteert. We hebben in 2024 geen melding ontvangen via deze opengestelde weg.

Gemeentelijke informatiebeveiliging

In 2024 is een VNG-aanbestedingstraject (GGI-veilig) doorlopen voor monitoring- en responsediensten. Voor de implementatie van deze diensten is een proof of concept gedraaid en is securitytoets op de staat van de informatiebeveiliging van de gemeente uitgevoerd. De hierbij geconstateerde mogelijke beveiligingsrisico's zijn in beeld gebracht en maatregelen zijn doorgevoerd om deze te mitigeren. In het laatste kwartaal van 2024 zijn de diensten volledig geïmplementeerd. Dat betekent 24/7 detectie en snelle analyses van digitale dreigingen om in voorkomende gevallen direct te kunnen handelen.

Aanvullend is in 2024 gewerkt aan het regelen van een offline back-up. Een dergelijke back-up is essentieel omdat deze niet rechtstreeks verbonden is met de gemeentelijke "productie-omgeving". Mocht er sprake zijn van een grootschalig incident met ransomeware, kan deze back-up niet besmet raken en kan de gemeente haar data gemakkelijker terugzetten.

Bovenstaande activiteiten leveren een belangrijke bijdrage aan het verbeteren van de digitale weerbaarheid van onze gemeente. Toch is niet uit te sluiten dat de gemeente te maken krijgt met een grootschalig incident. De gemeente moet voorbereid zijn op het risico van uitval van gemeentelijke dienstverlening en de bedrijfsvoering. In 2024 is het beleidsplan bedrijfscontinuïteit geactualiseerd. In dit beleidsplan zijn de cruciale processen opgenomen die in geval van een cyberincident binnen 48 uur weer geleverd moeten worden. Al dan niet in een gewijzigde (minder digitale) vorm. Met het management is een cybercrisisoefening gedaan om feeling te krijgen bij wat er op de gemeente af kan komen tijdens een cyberincident. Het management moet zorgen voor continuiteïtsplannen voor de processen binnen de verschillende clusters.

In 2024 hebben medewerkers 28 keer een informatiebeveiligingsincident gemeld. 11 meldingen betroffen beveiligingslekken. Door dit te melden konden maatregelen doorgevoerd worden en zijn daadwerkelijke incidenten en eventuele datalekken voorkomen. De overige meldingen betreffen meldingen van incidenten met mogelijk onbeveoegde kennisname van persoonsgegevens (zie hoofdstuk 3, datalekken).

Melding incident of datalek	Beveiligingslek
28	11

Voorbereiding op nieuwe regelgeving: NIS2, cybersecuritywet en BIO2

In 2024 is een memo opgesteld en gedeeld met de raad over bovengenoemde nieuwe wetgeving. Kern van de boodschap is dat de gemeente digitaal weerbaar moet zijn, de digitale risico's worden steeds groter. Dit vergt telkens opnieuw aandacht en aanpassingen. Hackers zitten immers niet stil, beveiligingsmaatregelen moeten aangepast worden om voldoende weerbaar te blijven.

De herziene Europese Network and Information Security-directive, kortweg de NIS2-richtlijn, heeft als doel om de cyberweerbaarheid in EU-lidstaten te verbeteren. De Nederlandse uitwerking van deze wet heet de Cyberbeveiligingswet. Deze zal naar verwachting het 3e kwartaal van 2025 ingaan. Voor gemeenten geldt dat zij dan moeten (gaan) voldoen aan de nieuwste versie van de BIO 2.0(1) waarin de verscherpte beveiligingsmaatregelen volgens NIS 2 zijn opgenomen.

De gemeente werkt met een ISMS (information security management system) waarin op maatregelenniveau is opgenomen in hoeverre de gemeente voldoet aan de beveiligingsmaatregelen en waar verbetering nodig is. In dit systeem worden ook de gemelde informatiebeveiligingsincidenten en datalekken geregistreerd. In 2024 is het geheel aan ICT beveiligingsmaatregelen door de adviseur Informatieveiligheid doorgenomen ter voorbereiding op de implementatie van de Cyberbeveiligingswet en de verscherpte maatregelen in de baseline informatieveiligheid. Daarnaast is gestart met het opstellen van een proces voor de verplichte registratie en de meldplicht van grootschalige incidenten bij de toezichthoudende autoriteit (Rijksinspectie Digitale Infrastructuur).

ENSIA en andere kwaliteitsaudits

Jaarlijks wordt een proces van zelfevaluatie op de informatiebeveiliging doorlopen. Daarnaast wordt jaarlijks een externe DigiD-audit en audit op Suwinet-inkijk uitgevoerd. Deze externe audits zijn met goed gevolg doorlopen. Hierover is apart gerapporteerd via een collegeverklaring, zowel richting de gemeenteraad als richting toezichthoudende organisaties. Er is weer geaudit op de regels van de BRP en reisdocumenten via het invullen van een kwaliteitsmonitor. Ook zijn de zelfaudits voor de overige basisregistraties zoals BAG, BGT en BRo weer doorlopen. De scores zijn goed. Er zijn de afgelopen jaren veel verbeteringen doorgevoerd, ook om de continuïteit van het beheer te verbeteren. Verbeteringen die nu genoemd zijn, zijn vooral gericht op het actueel houden van verschillende handboeken/ procedures.

3. Privacy

Geldende kaders privacy: (u) AVG

Een gemeente beschikt over veel persoonsgegevens van haar inwoners, ondernemers en samenwerkingspartners. Gemeenten moeten voorzichtig zijn met de (digitale) persoonsgegevens die zij verzamelen en beheren om de privacy van haar inwoners, ondernemers en medewerkers te waarborgen. De regels hiervoor liggen vast in Europese Regelgeving; de AVG die sinds 25 mei 2018 van kracht is, en de Nederlandse uitwerking daarvan.

Borging AVG in organisatie

De gemeente heeft strategisch privacybeleid vastgelegd. In dat beleid is opgenomen dat de gemeente voldoet aan de (u)AVG. En dat deze wetgeving ook van toepassing is voor het gebruik van Algoritmes en AI. Tevens wordt verwezen naar de verschillende materiewetten waarin soms ook specifieke eisen worden gesteld.

Er is een Functionaris Gegevensbescherming (FG) aangesteld en aangemeld bij de Autoriteit Persoonsgegevens. De privacyadviseur is eerste adviseur voor management en medewerkers als het gaat over het voldoen aan de privacywetgeving. De adviseur heeft een coördinerende rol in het jaarlijks actualiseren van het verwerkingenregister. De adviseur helpt en adviseert onder andere bij het opstellen of actualiseren van de privacy impact analyses (DPIA) en alle voorkomende vraagstukken op het gebied van privacy.

Er is in 2024 gestart met een inventarisatie van de '*must have DPIA's*' zoals door de IBD zijn gedeeld. Een gemeente moet minimaal de DPIA's hebben geregistreerd van alle gegevensverwerkingen waar sprake is van een hoog privacy risico en dient deze eveneens periodiek te actualiseren. Van een hoog privacy risico is sprake wanneer er heel veel persoonsgegevens worden geregistreerd en wanneer er zeer gevoelige gegevens worden bijgehouden over personen. Er is geconstateerd dat er soms wel een aanvang met deze analyses is gemaakt, maar dat deze niet altijd definitief gemaakt zijn. Ook is er te weinig toegezien op het uitvoeren van de verbetermaatregelen die uit de DPIA's komen. Hierop zijn de verantwoordelijke managers gewezen.

Er zijn nieuwe door de IBD gedeelde sjablonen voor deze DPIA's met instructies doorgevoerd. We verwachten dat deze verbeteringen het gemakkelijker maken om een DPIA uit te voeren. De melding van datalekken door medewerkers is toegankelijker gemaakt door het ontwikkelen van een formulier op het intranet. Hiermee zijn direct alle vragen die nodig zijn om het lek te analyseren inzichtelijk. In de hierbij horende geactualiseerde procedures is ook controle en toezien op invoering van de maatregelen opgenomen.

Rechten van betrokkenen

In 2024 zijn de procedures voor inzageverzoeken geactualiseerd. De gemeente heeft van drie personen inzageverzoeken op grond van de AVG ontvangen. Een van deze betrokkenen heeft ons meerdere verzoeken gestuurd en meerdere keren gevraagd om al zijn gegevens te wissen en te anonimiseren. Deze verzoeken zijn in 1x afgehandeld. Twee verzoeken zijn toegekend, een verzoek is deels toegekend omdat de gemeente een aantal documenten in overeenstemming met Archiefwet nog moet bewaren.

Datalekken

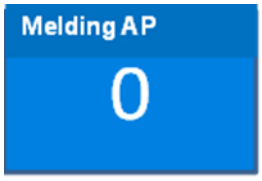
Het aantal meldingen van datalekken is in de afgelopen jaren iets opgelopen. Dat kan ook positief zijn, omdat er meer aandacht is gevraagd bij medewerkers voor het melden. Medewerkers lijk zich meer bewust van het feit dat datalekken gemeld moeten worden. In 2024 zijn 17 (potentiële) datalekken gemeld door onze medewerkers en eventueel andere betrokkenen.

Noordoostpolder wijkt niet af van de landelijke trend. Nog steeds zijn de meest voorkomende datalekken:

- E-mail of brief naar een verkeerd (e-mail) adres.
- E-mail of brief bevat een verkeerde bijlage met persoonsgegevens van andere personen.
- Onjuiste autorisatie van een (enkele) medewerker tot systemen of zaken met risico op onbevoegde kennisname van persoonsgegevens.
- Documenten met persoonsgegevens bij de printer gevonden.
- Gescand document intern naar de verkeerde collega gestuurd

In alle gevallen betrof het persoonsgegevens van een of enkele personen en ook een zeer beperkt aantal persoonsgegevens. Telkens is de afweging gemaakt of er een melding aan de Autoriteit Persoonsgegevens en eventueel aan betrokkenen nodig was. Omdat er vaak sprake was van een onjuiste maar wel betrouwbaar[2] geachte ontvanger, was melden aan de Autoriteit niet nodig. We zien dat medewerkers wanneer zij ontdekken dat iets niet goed gegaan is, vaak zelf al aan de betrokkenen gemeld hebben dat er per ongeluk gegevens naar een verkeerde ontvanger zijn gestuurd. Dit heeft niet geleid tot privacyklachten bij de Functionaris Gegevensbescherming.

[2] Een medewerker van de gemeente die ambtenaren eed en integriteitsverklaring heeft afgelegd of een externe partij waarmee we zakendoen en afspraken hebben over geheimhouding.


Melding AP
0

4. Wet Politiegegevens

Wanneer een gemeente haar taken uitvoert en daarbij persoonsgegevens verwerkt, is de Algemene Verordening Gegevensbescherming (AVG) altijd van toepassing. Maar als een Buitengewoon opsporingsambtenaar (BOA) persoonsgegevens verwerkt, dan ligt dat soms net even anders. Die gegevens kunnen namelijk onder verschillende wettelijke regimes vallen. Persoonsgegevens die een boa verwerkt in zijn rol als toezichthouder, vallen onder de AVG. De gegevens die de boa als opsporingsambtenaar verwerkt, vallen onder de Wet politiegegevens (Wpg).

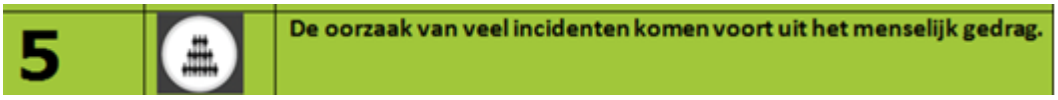
De Wpg is voor de gemeente van toepassing voor de Boa's en de leerplichtambtenaren. Hierop wordt verplicht geaudit op opzet, bestaan en werking: een maal per 4 jaar een externe audit en de overige jaren een interne audit. De jaarlijkse interne audit heeft betrekking op één dan wel een aantal onderdelen van de wet. De verplichte externe volledige audit zal over het jaar 2025 weer plaatsvinden in 2026. In 2024 richtte de interne audit zich op het onderdeel leerplicht:

- Het handhaven bij verwijtbaar schoolverzuim
- Het opmaken van een proces verbaal.

De bevindingen op dit specifieke onderdeel zijn gepresenteerd met als aanbeveling om in de werkinstructie of handboek van de leerplichtambtenaren nadrukkelijker aandacht te schenken aan de eisen die vanuit de Wpg aan hun werkzaamheden worden. Hierin moet aandacht zijn voor het onderscheid tussen feitelijke gegevens en persoonlijke oordelen. Er is geen procedure voor het vernietigen of het rectificeren van politiegegevens, dat is wettelijk verplicht en moet opgesteld en uitgevoerd gaan worden. De aanbeveling is gedaan om in de werkprocessen de toezichthoudende rol van de Functionaris Gegevensbescherming te borgen, zodat deze de beschreven controles kan uitvoeren.

We zien op het gebied van de Wpg dat de organisatie vanaf 2023 stappen maakt om op beide domeinen te voldoen aan de Wpg. Er zijn na de eerste verplichte audit op basis van verbeterplannen en extra (interne) audits aanzienlijke verbetering doorgevoerd. Er is zicht op waar nog aanscherpingen nodig zijn.

5. Bewustwording medewerkers



Menselijk handelen speelt een belangrijke rol in het veilig houden van de (persoons)gegevens die de gemeente beheert. Mochten alle technische maatregelen falen vormen de medewerkers de laatst 'buffer'. Alert handelen en melden van onregelmatigheden is van groot belang. Voortdurende bewustwording en training op het gebied van informatiebeveiliging en privacy is dan ook belangrijk. Daarom wordt er in de gemeente, naast de verantwoordelijkheid van het management hierin, door een aparte werkgroep aandacht gevraagd voor veilig en privacybewust handelen.

Er worden periodiek berichten op het intranet geplaatst zowel over informatieveiligheid als over het belang van het waarborgen van privacy. Aanvullend daarop is in 2024 voor de medewerkers een cybersecuritykwis georganiseerd. Daarbij is op een ludieke wijze aandacht gevraagd voor dit onderwerp. Het management is op de hoogte gebracht over de aanpassingen in procedures en afspraken. Ook is met hen van gedachten gewisseld over hun rol bij het bewust afwegen van het belang van privacy van onze inwoners versus bedrijfsbelang.

De toename van (sms en whatsapp) phishing is ook zichtbaar bij onze gemeente. Meer collega's melden dat ze berichten ontvangen op hun telefoon. Maar het grootste risico zit nog steeds in e-mails die steeds minder goed te onderscheiden zijn van echt. Dat is terug te zien in het aantal waarschuwingsberichten via het intranet en e-mail. Medewerkers worden snel geattendeerd op actuele dreigingen, zoals CEO-phishing[3].

Nieuwe medewerkers hebben de verplichting om binnen 3 maanden na indiensttreding een training te volgen. Het volgen van de training wordt geregistreerd. In 2024 is met HR besproken dat de groep externe medewerkers eveneens deze training moeten volgen. Ook is onderzocht hoe vaak een herhalingstraining ingevoerd moet worden. Daarnaast zijn er bij alle introductiedagen workshops gegeven aan nieuwe medewerkers over informatieveiligheid en privacy. De Wet Politiegegevens wordt hierin ook meegenomen.

[3] Fraudeurs doen zich voor als personen met een hoge functie binnen de organisatie, zoals directie en bestuurders