Toezichtjaarverslag CISO en FG 2023

Lotte Schieving - FG
Wessel Hemels - CISO

Inhoud

1. Inleiding en samenvatting

Gemeenten gebruiken informatie en persoonsgegevens van inwoners om hun taken uit te voeren. Ze gebruiken niet alleen gegevens van inwoners, maar ook van medewerkers en relaties van de gemeente. De Baseline Informatiebeveiliging Overheid (BIO), de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg) geven waarborgen voor het beschermen van deze gegevens. Zij verplichten organisaties aantoonbaar maatregelen te nemen om informatiebeveiliging en privacy te waarborgen. Iets waar de aanstaande Europese Network and Information Security (NIS2)-richtlijn (eind 2024) ook op zal toezien. Onjuist en onzorgvuldig gebruik van gegevens kan grote gevolgen hebben voor mensen en kan het vertrouwen in de gemeente en haar bestuurders schaden. De toeslagenaffaire laat zien hoe ingewikkeld problemen door onzorgvuldig gegevensgebruik kunnen worden. Voor medewerkers van de gemeente kunnen incidenten met gegevens grote gevolgen hebben. De organisatie is soms weken, zo niet maandenlang, bezig met de nasleep van zo'n incident. Niet voldoen aan de AVG en de Wpg kan bovendien leiden tot boetes van de Autoriteit Persoonsgegevens (AP) en schadeclaims van personen.

De Chief Information Security Officer (CISO) en de Functionaris voor Gegevensbescherming (FG) zijn onafhankelijke interne toezichthouders voor informatiebeveiliging en privacy. De CISO controleert de naleving van de BIO bij het gebruik van informatie. De FG houdt toezicht op de naleving van de AVG en de Wpg bij het gebruik van persoonsgegevens en politiegegevens. In 2023 hebben de CISO en de FG de voortgang van de acties uit het Privacy- en informatiebeveiligingsplan in de gaten gehouden. Naast geplande werkzaamheden hebben ze ook hun bevindingen gedeeld bij incidenten of adviesvragen. In dit toezichtjaarverslag brengen de CISO en de FG verslag uit aan de colleges van de gemeenten Deventer, Olst-Wijhe en Raalte over de gegevensverwerkingen die onder hun verantwoordelijkheid vallen. Het verslag geeft geen definitief oordeel over de mate waarin de gemeenten op dit moment aan de regels uit de BIO, AVG en Wpg voldoen. Wel geeft het een beeld van de stand van zaken bij de drie gemeenten in 2023.

Het verslag begint met wat de CISO en de FG in 2023 hebben opgemerkt. Ze zien dat sommige problemen die ze eind 2022 en 2021 hebben gesignaleerd, zijn opgelost. In 2023 is er, net zoals in voorgaande jaren, hard gewerkt aan het verbeteren van informatieveiligheid en privacy in de drie organisaties. Er zijn daarbij stappen gezet in het verder inbedden van het informatiebeveiliging- en privacymanagement. Bijvoorbeeld bij het inrichten van het proces voor het uitvoeren van DPIA's, het

opzetten van een tool voor de registers van verwerkingen en het opstellen van een plan van aanpak voor de implementatie van de Wpg. Een groot deel van de gesignaleerde problemen vraagt echter ook in 2024 nog aandacht. In dit verslag worden per aandachtsgebied zowel de positieve ontwikkelingen als de risico's besproken, samen met aanbevelingen voor 2024. Deze zien er als volgt uit:

Governance

- Verhoog het bewustzijn in de organisaties als het gaat om de rollen bij informatiebeveiliging en privacy (three lines of defense model)
- Verbeter de betrokkenheid van de organisaties bij gemeentebrede acties voor informatieveiligheid en privacy in DOWR-verband
- Bundel (waar mogelijk) adviezen vanuit informatiebeveiliging en privacy aan het management met adviezen uit de andere informatiegebieden
- Maak periodiek sturingsinformatie beschikbaar aan de organisaties en bespreek dit met bestuur en directie
- Bewaak de onafhankelijke positie van derde lijns- functionarissen (CISO en FG)
- Professionaliseer de functie van de CISO en de FG

Privacy en security by design

- Werk achterstanden bij het uitvoeren van risicoanalyses voor privacy (DPIA’s) en informatiebeveiliging (DRA’s) weg en geef prioriteit aan deze werkzaamheden vanuit de teams en domeinen
- Breng de praktijk bij DPIA’s in lijn met de opgestelde procedure
- Zorg voor voldoende kennis en begrip van processen in de organisaties, zodat er gestuurd kan worden op gegevensverwerkingen in informatieketens en werkprocessen
- Zorg dat DPIA’s en DRA’s centraal beschikbaar zijn en bewaak de resultaten

Overzicht creëren

- Werk zo snel mogelijk de drie registers van verwerkingen bij en richt dataclassificatie in
- Besteed aandacht aan de capaciteit in de teams en domeinen bij de actualisatieslag
- Draag zorg voor het bijhouden van de geregistreerde werkprocessen en informatiesystemen

Incidenten

- Deel lessen en ervaringen bij incidenten breed binnen de organisaties
- Dring schaduw IT terug doormiddel van duidelijke afspraken
- Zorg voor een integrale aanpak van informatiebeveiliging en privacy bij de aanschaf van applicaties en diensten

Bewustwording

- Vergroot planmatig het bewustzijn en gebruik verschillende soorten 'bewustwordingsprikkels'
- Dring er bij managers op aan dat zij privacy en informatiebeveiliging als integraal onderdeel van de werkprocessen naar medewerkers uitdragen

Rechten van betrokkenen

- Neem in de privacyverklaringen op hoe gemeenten omgaan met politiegegevens
- Vraag in de organisaties aandacht voor de taken en verantwoordelijkheden bij AVG- of Wpg-verzoeken

Auditverplichting Wet politiegegevens

- Start met verbeterplannen en besteed aandacht aan capaciteit in de teams bij de benodigde acties

Wet beveiliging netwerk- en informatiesystemen (Wbni)

- Besteed aandacht aan de capaciteit bij de inzet van de informatiebeveiligingsfunctionarissen (ISO, TISO en CISO) voor de implementatie van de NIS2-richtlijn (Wbni)

Vervolgens bespreken de CISO en de FG in dit verslag ontwikkelingen die in 2024 extra aandacht vragen van de drie organisaties. Het verslag eindigt met een conclusie.

2. Aandachtsgebieden

2.1 Governance

In het privacybeleid van de gemeenten is vastgelegd hoe de organisatiestructuur voor informatiebeveiliging en privacy is opgebouwd volgens het *three lines of defense* model. Het management is verantwoordelijk voor het naleven van informatiebeveiliging en privacy in de werkprocessen. De Privacy officers (PO's) en de Information security officers (ISO's) vormen de tweede lijn en ondersteunen en adviseren het management. In 2023 zijn er 2 nieuwe PO's aangetrokken, die in mei zijn gestart. De derde lijn, bestaande uit de CISO en FG, houdt toezicht op de naleving van informatiebeveiliging en privacy in de drie gemeenten. In de praktijk wordt deze structuur niet altijd even goed gevolgd. Bij sommige onderwerpen zijn de ISO en de PO duidelijk gesprekspartners van het management, zoals bij het melden van incidenten. Maar bij andere onderwerpen vinden de eerste en tweede lijn elkaar niet of niet op tijd, zoals bij het laten beoordelen van nieuwe initiatieven. Dit duidt op een gebrek aan bewustzijn in de organisaties om de toegewezen rollen te vervullen. De afstand tussen het management en de in DOWR-verband opererende functionarissen voor informatiebeveiliging en privacy kan hierbij een rol spelen.

Op dit moment zijn er een aantal belangrijke overleggen voor informatiebeveiliging en privacy. Er is een wekelijks privacyoverleg tussen de FG en de PO's en een wekelijks overleg voor informatiebeveiliging en privacy waar ook de CISO aan deelneemt. Deze overleggen zijn informeel en hebben geen officiële status als opstap naar andere overleggen. Ze richten zich vooral op het bespreken van lopende zaken en het delen van kennis. Deze overleggen worden als waardevol gezien voor beide vakgebieden, omdat ze de samenwerking versterken. Vooral op punten waar gedeelde belangen spelen, zoals bij bewustwording. In Deventer nemen de CISO en de FG deel aan het Strategisch informatieoverleg (SIO), terwijl dit bij Olst-Wijhe en Raalte niet het geval is. Het SIO in Deventer wordt gebruikt om informatiebeveiliging en privacy onderdeel te laten worden van de meerjarige informatiemanagementstrategie. In Raalte nemen de ISO en PO deel aan het Kernteam informatiemanagement (het operationeel informatieoverleg, het OIO) en het tactisch informatieoverleg (TIO) terwijl dit bij Deventer en Olst-Wijhe niet het geval is. Het Kernteam overleg in Raalte wordt gebruikt om informatiebeveiliging en privacy mee te laten nemen als onderdeel van de ontwikkelingen in de domeinen. In dit overleg zijn alle domeinen vertegenwoordigd. Hier wordt onder andere de behoefte aan praktische handvatten voor informatieveiligheid en privacy besproken. Het TIO in Raalte wordt gebruikt voor het afstemmen van acties binnen de vakgebieden privacy, informatiebeveiliging en informatiebeheer. Het advies is om in 2024 ook in de andere gemeenten de CISO en de FG deel te laten nemen aan het SIO en de ISO en de PO deel te laten nemen aan het OIO en het TIO. Dit kan ook een soortgelijk overleg zijn.

Vaak hebben de ISO en PO veel contact met medewerkers uit de informatiekolom als het om gemeente brede risico's gaat. Ze stemmen acties af met de CISO en de FG en communiceren dit naar de organisaties, maar de betrokkenheid binnen de organisaties zelf is beperkt. Het wordt aanbevolen om dit in 2024 te verbeteren. Het actualiseren van het privacybeleid uit 2018 kan daarbij helpen. Zowel de AVG als de Wpg vragen om een actueel privacybeleid. Zo kunnen de verantwoordelijkheden bij specifieke onderwerpen opnieuw onder de aandacht worden gebracht bij het bestuur, de directie en het management. Informatie over de voortgang op het gebied van informatiebeveiliging en privacy belandt vaak toevallig op de bestuurs- en directietafels in de drie gemeenten. Dit betekent dat alleen de functionarissen bij informatiebeveiliging en privacy zicht hebben op hoe de organisaties ervoor staan als het gaat om de BIO, de AVG en de Wpg. Het is aan te raden om deze sturingsinformatie periodiek beschikbaar te stellen aan de organisaties en hierover met het bestuur en de directie in gesprek te gaan. Dit maakt ook duidelijker op basis van welke informatie de (jaarlijkse) aanbevelingen van de CISO en de FG tot stand komen.

De gebieden informatiemanagement, informatiebeveiliging, privacy en datamanagement zijn sterk met elkaar verbonden en overlappen op verschillende onderwerpen. Hierdoor bestaat het risico dat de eerste lijns- manager overladen wordt met verschillende adviezen vanuit verschillende invalshoeken. Het directiebesluit over de rol van de Chief Information Officer (CIO) beschrijft hoe het CIO-bureau bij de gemeente Deventer wordt opgezet. In 2024 worden de CISO, de ISO's, de FG en de PO's ondergebracht in het CIO-bureau. Positief is dat de gemeente Deventer met het CIO-bureau probeert de samenwerking tussen verschillende tweede lijns- informatiefuncties te versterken, zoals

de ISO's, de PO's, de CIO, de strategisch informatiemanager Deventer en de business architect Deventer. In 2024 is het aan te raden dat de drie gemeenten bij het verder ontwikkelen van de organisaties rekening houden met de samenhang tussen verschillende informatiedomeinen (waaronder ook informatiebeheer). Dit punt valt voor een deel buiten het bereik van de aanpak voor informatiebeveiliging en privacy en moet ook door de organisaties zelfstandig worden opgepakt.

Het lijkt minder logisch om de CISO en de FG binnen het CIO-bureau te plaatsen. Dit sluit niet goed aan bij het *three lines of defense* model, waarin de CISO en de FG onafhankelijk als derde lijn moeten opereren ten opzichte van de drie organisaties. Het is belangrijk dat deze verplaatsing geen beperkingen oplevert in de directe lijnen naar bestuur, directie en raad in Deventer, Olst-Wijhe en Raalte. Nu deze verandering wordt doorgevoerd, is het essentieel om zorgvuldig te kijken naar de waarborgen die daarbij moeten gelden. Ook moet worden onderzocht wat de verplaatsing naar het CIO-bureau betekent voor de budgetten bij informatiebeveiliging. Daarnaast wordt de CIO volgens het directiebesluit als proceseigenaar verantwoordelijk voor de verwerking van persoonsgegevens in het nieuw op te zetten datateam (GEO en KV), dat onderzoeken uitvoert voor Deventer en Olst-Wijhe. Dit vraagt om duidelijke afspraken tussen de CIO, CISO en FG over hoe zij omgaan met onafhankelijk advies richting de CIO in zijn rol als manager in de eerste lijn. De directie in Deventer heeft aangegeven dat de verplaatsing van de functionarissen niets verandert aan de profielen van de FG, PO en ISO zoals die zijn opgesteld met het capaciteitsvoorstel van 2022.

De FG, de PO's en de CISO werken nauw samen. De CISO werkt voor 0.5 fte ook als ISO voor DOWR-i en de FG neemt naast haar werk financiële control werkzaamheden op zich. De CISO en de FG hebben opgemerkt dat deze dubbele rollen de scheiding tussen de tweede en de derde lijn voor informatiebeveiliging en privacy verzwakt. Vanwege de vraag vanuit de drie organisaties heeft de CISO in 2023 veel tijd moeten besteden aan adviserende taken in zijn rol als ISO. Hierdoor had hij te weinig tijd over voor zijn taken als CISO. Bovendien heeft hij vastgesteld dat hij de vraag naar zijn CISO-rol met 0.5 fte niet aankan. De PO's hebben op hun beurt aangegeven dat zij een volwaardige sparringpartner missen in de 0.5 fte ISO DOWR-i. Deze manier van werken maakt niet alleen de toetsende rol vanuit informatiebeveiliging lastiger uit te voeren, maar leidt ook tot de onwenselijke situatie dat de CISO soms zijn eigen werk moet beoordelen. Vooral bij taken als het uitvoeren van risicoanalyses, waar de scheiding tussen 2e en 3e lijn vervaagt. Bij de FG zien we iets soortgelijks gebeuren als zij financiële control taken op zich neemt. Dit komt voort uit haar rol bij het opstellen van het capaciteitsvoorstel voor privacy in 2022. De FG heeft goed inzicht in de financiële privacy constructies bij de drie gemeenten. Ze ondersteunt daarom bij het beheren van de privacy budgetten en voorziet in de financiële informatievoorziening richting de gemeenten. Deze werkzaamheden voert ze uit naast haar toezichthoudende taak waarbij zij ook toeziet op deze privacy werkzaamheden. De mate waarin dit als problematisch wordt ervaren in de organisaties hangt vooral af van hoe de CISO en de FG nu zelf de verschillende rollen naast elkaar invullen. De CISO en de FG hebben recent aangegeven dat de grens bereikt is en dat zij behoefte hebben aan een strakkere inrichting van het *three lines of defense* model. Het advies is om de functie van de CISO en de FG verder te professionaliseren en als gemeenten te benadrukken dat er waarde gehecht wordt aan deze toezichtrollen op gemeenteniveau. Een bijkomend voordeel is dat de huidige 0,5 fte DOWR-i ISO functie dan als 1,0 fte kan worden ingevuld.

2.2 Privacy en security by design

Data protection impact assessment (DPIA's)
Gemeenten moeten privacy risicoanalyses (DPIA's) uitvoeren wanneer zij persoons- of politiegegevens gebruiken in werkprocessen met een mogelijk hoog privacyrisico. Bij een DPIA wordt beoordeeld wat de impact op de betrokkene is (de persoon over wie de gegevens gaan) en worden eventuele privacyrisico's aangepakt. In 2023 heeft de AP opnieuw benadrukt hoe belangrijk DPIA's zijn door de gemeente Eindhoven onder verscherpt toezicht te plaatsen. Deze gemeente verzuimde DPIA's uit te voeren waar dat wel verplicht was. Zelfs na meerdere waarschuwingen van de FG. Begin 2024 kreeg International Card Services B.V. (ICS) verder een boete van 150.000 euro van de AP omdat ze op grote schaal persoonsgegevens gebruikte zonder eerst een wettelijk verplichte DPIA uit te voeren.

In de drie gemeenten zijn nog steeds veel wettelijke verplichte DPIA's niet uitgevoerd, naar schatting 150 (verdeeld over de drie gemeenten). Het is nog niet zeker of de lijst met vereiste DPIA's volledig

is, hoeveel daarvan betrekking hebben op *persoonsgegevens* en hoeveel op *politiegegevens*. In 2023 zijn in totaal 5 privacybeoordelingen (DPIA's) afgerond, maar zijn ook nieuwe werkprocessen bij de PO's aangemeld voor een privacybeoordeling. De werkachterstand bij de drie gemeenten is daarmee ongeveer hetzelfde gebleven als in 2022. Het niet in kaart hebben van de privacyrisico's bij werkprocessen is een groot punt van zorg. Deze tekortkoming wordt al vanaf 2018 gesignaleerd. Het uitbreiden van het privacyteam in 2023 kan alleen helpen bij het inhalen van de werkachterstanden als de teams en domeinen hier voldoende uren voor vrijmaken. Dit is ook van belang om onnodig lange doorlooptijden te voorkomen. Het gaat gemiddeld om 13 uur per DPIA en een doorlooptijd van 6 weken. Het is aan te raden dat proceseigenaren in 2024 keuzes maken over het plannen en prioriteren van de benodigde werkzaamheden. Het uitbreiden van de privacy capaciteit kan verder alleen helpen bij het wegwerken van de achterstanden als de 1,6 fte ISO (vanuit het capaciteitsvoorstel) in 2024 door de organisaties wordt ingevuld.

In 2023 heeft het privacyteam een procedure opgesteld voor het uitvoeren van DPIA's bij de drie gemeenten. Het advies is om specifiek de verwerking van politiegegevens en het uitvoeren van de Wpg aan deze procedure toe te voegen. De praktijk van het uitvoeren van DPIA's komt nog niet overeen met de beschreven procedure. In sommige gevallen meldt de proceseigenaar niet op tijd aan de PO dat er een nieuw werkproces is of een wijziging in een bestaand werkproces. Ook beseft de proceseigenaar zich niet altijd dat de beoordeling van een DPIA, budget en inzet van medewerkers vraagt. Hierdoor wordt een DPIA soms uitgesteld, pas uitgevoerd nadat een applicatie in gebruik is genomen of wanneer de gegevensverwerking al begonnen is. Vaak heeft men dan alleen naar de efficiënte uitvoering van de taken gekeken, zonder rekening te houden met informatiebeveiliging en privacy. Het is belangrijk om in deze situaties de directies te informeren, net zoals bij situaties waarin de kosten van de DPIA niet zijn begroot. Dit kan namelijk de ambitie van de directies om de werkachterstanden weg te werken in gevaar brengen. Een uitdaging is ook dat proceseigenaarschap vaak formeel aan één team, domein of programma is toegewezen, terwijl de gegevens waarvoor een DPIA wordt uitgevoerd, door meerdere teams, domeinen of programma's lopen. Het advies is om in 2024 als organisaties te investeren in voldoende kennis en begrip van processen. Zodat niet alleen de PO's een overzicht krijgen van de gegevensstromen, maar dat er ook daadwerkelijk iemand is die op gegevens in werkprocessen en ketens gaat sturen. Alleen op die manier kunnen procesverantwoordelijkheden, zoals het prioriteren van DPIA-werkzaamheden en het implementeren van beheersmaatregelen op basis van DPIA's, worden toegewezen en nagekomen. Dit punt valt voor een deel buiten het bereik van de aanpak voor informatiebeveiliging en privacy en moet ook door de organisaties zelfstandig worden opgepakt.

Een belangrijke stap bij het uitvoeren van DPIA's is het vastleggen en opvolgen van de resultaten. In 2023 heeft de FG een steekproef gedaan bij 10 DPIA's van verschillende teams en domeinen. In de helft van de gevallen waren de resultaten van de DPIA niet centraal geregistreerd. In alle gevallen heeft er geen monitoring plaatsgevonden op de resultaten. Het is onduidelijk of de resultaten vanaf 2021 zijn geïmplementeerd. Het advies voor 2024 is om ervoor te zorgen dat de DPIA's centraal beschikbaar zijn en monitoring plaatsvindt van de geplande maatregelen. Anders kan het doel van een DPIA, namelijk het daadwerkelijk implementeren van waarborgen in het werkproces, mogelijk niet worden bereikt.

Baselinetoetsen BBN en Diepgaande Risicoanalyses (DRA's)

Baselinetoetsen BBN en Diepgaande Risicoanalyses (DRA's) zijn belangrijke instrumenten voor gemeenten om informatiebeveiligingsrisico's in kaart te brengen en maatregelen te treffen. Dit is vooral belangrijk bij het gebruik van gevoelige informatie in werkprocessen. Deze toetsen moeten regelmatig en gemeente breed worden uitgevoerd, vergelijkbaar met DPIA's op persoons- en politiegegevens. Hoewel de ISO in 2023 processen en applicaties heeft getoetst, is er vanwege personele beperkingen nog niet voldoende capaciteit om dit te doen voor alle processen en applicaties. Dit brengt met zich mee dat de gemeenten onvoldoende inzicht hebben in hun informatiebeveiligingsrisico's.

In 2023 heeft de CISO een steekproef uitgevoerd bij kritische applicaties van DOWR. Hierbij is gebleken dat sommige daarvan niet voldoen aan de vereiste basisbeveiliging volgens de Baseline Informatiebeveiliging Overheid (BIO). Dit brengt risico's met zich mee voor de betrouwbaarheid en de bescherming van de informatie die door deze applicaties wordt verwerkt. Het advies voor 2024 is om de achterstanden bij de BBN-toetsen en DRA's weg te werken en dit proces te borgen door middel van het inrichten van risicomanagement.

2.3 Overzicht creëren

Register van verwerkingen

Volgens de AVG en de Wpg moeten gemeenten een overzicht bijhouden van structurele werkprocessen waarin persoons- of politiegegevens worden gebruikt. Dit overzicht, ook wel een verwerkingsregister genoemd, geeft inzicht in hoe en waarom bepaalde gegevens binnen de gemeente worden gebruikt. In 2018 zijn de werkprocessen met *persoonsgegevens* in de registers van de drie gemeenten opgenomen en daarna niet meer bijgewerkt. Dat betekent dat op dit moment niet zeker is of de beschrijving daarvan nog juist en volledig is. Bovendien zijn de werkprocessen met *politiegegevens* in 2018 helemaal niet opgenomen. Dit heeft als gevolg dat bij een beveiligingsincident (potentieel datalek) niet naar de registers gekeken kan worden voor informatie. Het register zou bijvoorbeeld kunnen aangeven welke applicaties er bij een werkproces betrokken zijn en welke gegevens een rol spelen. Organisaties moeten wettelijk binnen 72 uur een ernstig datalek melden aan de AP. Het ontbreken van informatie kan leiden tot vertraging bij het inschatten van de aard en omvang van een incident.

In 2024 wordt er een externe partij ingeschakeld om de registers te actualiseren. Er wordt tijdelijk een ingehuurde PO toegevoegd aan het bestaande privacyteam. Deze PO begeleidt medewerkers bij het (aan)vullen van de registers en heeft daarvoor informatie nodig vanuit de werkprocessen. Alleen medewerkers in de teams en domeinen kunnen aangeven of de beschrijvingen in de registers verouderd zijn, moeten worden veranderd of dat er nieuwe werkprocessen moeten worden toegevoegd. Ook weten zij waar in de organisaties werkprocessen voorkomen waarin politiegegevens worden gebruikt. Het is nog niet duidelijk of medewerkers over voldoende capaciteit beschikken om de benodigde informatie te verstrekken en of de proceseigenaren de urgentie voelen om aan de registerverplichting te voldoen. Het advies is om hier in 2024 als organisaties aandacht aan te besteden, omdat dit belangrijk is voor het succes van de actualisatie.

In 2023 is er een verwerkingsregister-tool in SharePoint ontwikkeld. Alle werkprocessen met persoons- en politiegegevens worden in één register per organisatie vastgelegd. Het gebruik van één systeem door de drie organisaties zorgt voor consistentie en standaardisatie in de vastlegging. In de tool kunnen ook verwijzingen naar bestaande stukken worden opgenomen, zoals risicoanalyses (DPIA's). De tool wordt daarmee ook een centrale plek voor de privacy administratie. Medewerkers en proceseigenaren krijgen toegang tot het register, zodat zij daar hun werkprocessen kunnen bekijken. In 2024 zal de gebruiksvriendelijkheid van de tool worden getest en de tool worden gevuld. Het is aan te raden minstens elke 2 jaar proceseigenaren te vragen hun werkprocessen opnieuw te controleren. Zo wordt voorkomen dat het bijwerken van de registers wordt vergeten zodra de actualisatie is afgerond.

Dataclassificatie

Dataclassificatie is een manier om de gegevens die we binnen de gemeenten gebruiken, in te delen op basis van hoe belangrijk en gevoelig ze zijn. Het idee is om verschillende niveaus van bescherming toe te passen op verschillende soorten informatie. Informatie kan worden ingedeeld in drie categorieën:

- Openbaar: Dit zijn gegevens die voor iedereen toegankelijk zijn en geen schade aanrichten als ze openbaar worden.
- Intern: Deze gegevens zijn bedoeld voor gebruik binnen de gemeenten en zijn niet bedoeld om met iedereen te delen. Als ze wel lekken, veroorzaakt dit waarschijnlijk geen grote problemen.
- Vertrouwelijk: Dit zijn zeer gevoelige gegevens die we goed moeten beschermen. Het lekken van deze gegevens zou aanzienlijke schade kunnen veroorzaken. Hierbij kun je denken aan persoonlijke informatie, financiële gegevens, of belangrijke gemeentegeheimen.

Door te weten welke gegevens in welke categorie vallen, kunnen de juiste beveiligingsmaatregelen worden genomen. Dit omvat zaken zoals versleuteling, het beperken van toegang en het monitoren van wie toegang heeft tot welke informatie. Dit helpt niet alleen om de gegevens beter te beschermen, maar ook om te voldoen aan wetten en regels voor informatiebeveiliging en privacy.

In 2023 zijn de organisaties gestart met het toepassen van basis dataclassificatie voor gegevens op het Microsoft (Sharepoint) platform. Voor 2024 wordt geadviseerd om dataclassificatie verder vorm te geven en om te toetsen of de gehanteerde veiligheidsmaatregelen nog passen bij de niveaus die al

zijn bepaald. Dit kan worden getoetst door middel van de DRA's (diepgaande risicoanalyses) die hierboven zijn besproken.

2.4 Incidenten

Beveiligingsincidenten
In 2023 hebben we de gevolgen van schaduw-IT binnen de gemeenten ervaren. Het fenomeen schaduw-IT, waarbij technologieën worden gebruikt zonder formele goedkeuring, brengt niet alleen uitdagingen met zich mee voor de IT-afdeling, maar vormt ook aanzienlijke risico's voor privacy en informatiebeveiliging. Medewerkers lopen het risico op deze manier onbedoeld gevoelige informatie bloot te stellen aan ongeautoriseerde derden. Denk aan apps, software of apparaten die niet zijn beoordeeld zijn op privacy en informatiebeveiligingsrisico's. Hoewel er in 2023 geen directe schade werd toegebracht door schaduw-IT is er wel een urgentie om schaduw-IT terug te dringen. Het wordt aangeraden om dit aan te pakken door middel van een integrale benadering, het vaststellen van duidelijke afspraken met derde partijen/leveranciers en het vergroten van het bewustzijn onder medewerkers.

Datalekken
In 2023 ontstonden de meeste datalekken in de drie gemeenten opnieuw door 'verkeerd geadresseerde mail of post'. Dit kan vervelende gevolgen hebben, vooral als het om gevoelige informatie of kwetsbare personen gaat. Ongeveer een derde van de intern gemelde datalekken in 2023 had ernstige gevolgen kunnen hebben voor de betrokkene(n). Deze gevallen zijn besproken met de FG tijdens het wekelijkse privacy-overleg en gemeld bij de AP. Door een datalek wordt het bewustzijn binnen het getroffen team of domein aanzienlijk vergroot. Medewerkers worden zich meer bewust van de privacyrisico's bij hun werk. Om dit bewustzijn in de hele organisatie te vergroten, wordt aangeraden om in 2024 de lessen die bij datalekken worden geleerd meer te delen met de rest van de organisatie, Dit kan bijvoorbeeld door een teammanager of domeinmanager te vragen een intranetbericht te plaatsen waarin wordt gedeeld wat het incident met het team of domein heeft gedaan. Het is ook raadzaam om bestaande tools, zoals ZIVVER, te gebruiken om de mogelijke gevolgen van incidenten te beperken. Hoewel de procedure voor datalekken goed wordt nagevolgd, is deze nog niet ingericht op de Wpg. Het advies is om dit in 2024 aan te passen, evenals het meldingsformulier.

2.5 Bewustwording

In 2023 hebben de drie organisaties het bewustzijn rond informatieveiligheid en privacy vergroot door middel van Nanolearning. De deelnamepercentages varieerden van gemiddeld 60% aan het begin van het jaar tot 40% aan het einde van het jaar. De PO's en ISO hebben de complexe normen van de BIO, de AVG en de Wpg voor enkele teams en domeinen vertaald naar praktische richtlijnen voor dagelijks gebruik tijdens overleggen en bijeenkomsten. Een deel daarvan is te vinden op de nieuwe Sharepointpagina. Voor 2024 wordt aanbevolen om naast trainingen en workshops ook andere 'bewustwordingsprikkels' te gebruiken, zoals het versturen van nep-phishingberichten.

Uit de gesprekken met managers en medewerkers blijkt dat het kennisniveau per persoon verschilt en over het algemeen nog niet voldoende is. Soms worden risico's op het gebied van privacy of informatiebeveiliging door medewerkers op de werkvloer laat of zelfs niet herkend. Een uitdaging hierbij is de manier waarop het verhaal over informatiebeveiliging en privacy binnen de organisaties wordt verspreid. Momenteel wordt het vaak nog gezien als een belasting en 'iets dat je erbij moet doen', terwijl het eigenlijk een integraal onderdeel is van alle werkprocessen. De verantwoordelijkheden voor informatiebeveiliging en privacy liggen in de lijn. Medewerkers moeten in staat worden gesteld om er voldoende aandacht aan te kunnen besteden. De focus van de drie organisaties heeft de afgelopen jaren sterk op techniek en beveiliging gelegen in plaats van het inbouwen van waarborgen in *alle* werkprocessen. De directies kunnen hier in 2024 nadrukkelijk verandering in brengen door managers te vragen privacy en informatiebeveiliging op een andere manier richting hun medewerkers uit te dragen. Ook kan worden overwogen een trainingsprogramma binnen Nanolearning te ontwikkelen dat is gericht op het management.

2.6 Rechten van betrokkenen

De AVG en de Wpg geven personen verschillende privacyrechten. Deze rechten kunnen ze uitoefenen met betrekking tot hun *eigen* gegevens. Met het recht op inzage kunnen inwoners bijvoorbeeld informatie opvragen over hoe hun persoonsgegevens bij een gemeente worden gebruikt. De privacyverklaringen op de gemeentewebsites gaan in op de privacyrechten onder de AVG en geven aan hoe verzoeken bij de gemeenten kunnen worden ingediend. Het wordt aanbevolen om in deze verklaringen ook op te nemen hoe de gemeenten omgaan met politiegegevens onder de Wpg. Deze informatie mist nog.

In 2023 werd gemiddeld elke twee weken één verzoek ingediend met betrekking tot de uitoefening van privacyrechten in een van de drie gemeenten. AVG- of Wpg-verzoeken moeten binnen vier of binnen zes weken worden afgehandeld, afhankelijk van het soort verzoek. In bijna alle gevallen werd er binnen deze termijn gereageerd. Vaak was de persoon alleen bekend bij één team of domein en stonden de gegevens in slechts één informatiesysteem. Het aantal verzoeken nam in 2023 toe. Van ongeveer één verzoek per maand aan het begin van 2023 tot wekelijks één aanvraag. Bij de afhandeling van een groot inzageverzoek in de gemeente Deventer is er een handleiding gemaakt voor de teams en domeinen over het aanleveren van informatie. Ook zijn vragen gesteld aan het privacyteam over wie uiteindelijk beslist over het wel of niet in behandeling nemen van een verzoek. Het is aan te raden om met de drie organisaties te bespreken hoe de procedure bij de behandeling van een AVG- of Wpg-verzoek verloopt. Vooral als het gaat om de taken en verantwoordelijkheden van de PO's en de teams of domeinen. Het advies is om de procedure in 2024 op te nemen in een werkdocument en samen met de handleiding op Sharepoint beschikbaar te stellen.

2.7 Auditverplichting Wet politiegegevens

Sinds 2019 is de Wpg van kracht voor de het gebruik van politiegegevens bij gemeenten. Buitengewone opsporingsambtenaren (boa's) vallen onder de Wpg als ze politiegegevens gebruiken voor hun opsporingstaken. Onder de Wpg gelden strengere regels dan onder de AVG. Werkgevers van boa's moeten jaarlijks een interne Wpg-audit (zelfevaluatie) uitvoeren en elke vier jaar een externe Wpg-audit. Het resultaat van deze audit moet worden gedeeld met de AP. In 2022 heeft de externe audit laten zien dat er nog weinig actie is ondernomen om de Wpg in de werkprocessen te implementeren. De gemeenten hebben de AP hiervan op de hoogte gesteld. In 2023 heeft de PO een plan van aanpak voor de organisaties gemaakt. Dit plan wordt in 2024 ter goedkeuring bij de directies van Deventer en Olst-Wijhe voorgelegd. Het wordt aanbevolen om dit plan over te nemen. De gemeente Raalte heeft sinds maart 2023 geen boa's meer in dienst. Voor deze organisatie zal bekeken moeten worden wat deze verandering betekent voor de toepassing van de Wpg.

Voor de algemene aandachtspunten onder de Wpg, zoals het uitvoeren van DPIA's, zijn hierboven de bevindingen en aanbevelingen van de FG voor 2024 gegeven. Wat betreft de aandachtspunten die in de teams liggen, wordt geadviseerd om in 2024 te starten met de verbeterplannen. Het is daarbij belangrijk om te onderzoeken of de medewerkers in de teams voldoende capaciteit hebben om de benodigde acties uit te voeren.

3. Ontwikkelingen

Wet beveiliging netwerk- en informatiesystemen (Wbni)
Eind 2023 zijn de drie gemeenten begonnen met een nulmeting op het gebied van de ISO 27001-informatiebeveiligingsnorm. Dit onderzoek loopt door in 2024 en richt zich voorlopig alleen op de afdelingen PSA, DOWR-i en FZ. Het doel van de nulmeting is om te kijken waar de gemeenten momenteel staan en wat er nodig is om te voldoen aan deze internationale standaard. Op een later moment zal worden bepaald of het behalen van de ISO 27001-certificering wenselijk is. Dit zou de gemeenten voorbereiden op de aanstaande Network and Information Systems (NIS2)-richtlijn.

De NIS2-richtlijn is gericht op het beveiligen van netwerk- en informatiesystemen binnen de Europese Unie. Deze wordt eind 2024 omgezet naar Nederlandse wetgeving, de Wet beveiliging netwerk- en informatiesystemen (Wbni). Hierin wordt de BIO 2.0 opgenomen.

De nulmeting behandelt zowel de Wbni als de bredere context van de ISO 27001. Het uiteindelijke doel is niet alleen om aan de Wbni te voldoen, maar ook beheer van informatiebeveiliging te verbeteren en efficiënter te maken. Daarvoor wordt een Information Security Management System (ISMS) gebruikt. Het advies is om dit in 2024 verder in te richten.

De eisen van de BIO komen grotendeels overheen met wat de Wbni van de gemeenten vraagt. In 2024 moet er rekening worden gehouden met een grotere vraag naar de inzet van informatiebeveiligingsspecialisten (ISO, TISO, CISO). Ook zullen de organisaties moeten investeren in algemene, organisatie brede, kennis van informatiebeveiliging in het licht van deze nieuwe wetgeving.

Modern werken
De drie gemeenten willen meer applicaties lokaal toegankelijk maken op de moderne werkplek. Ondanks de voordelen van deze vernieuwende werkwijze, zoals meer flexibiliteit en mobiliteit, moeten ook de mogelijke risico's daarbij erkend worden. Voor 2024 is het advies zorgvuldig te bekijken hoe dit van invloed is op informatiebeveiliging en privacy.

De AP in 2024
Toezicht houden betekent keuzes maken. Het toezichtveld van de AP wordt namelijk steeds groter en de middelen zijn beperkt. De AP heeft in 2023 aangekondigd dat zij in 2024 extra aandacht zal besteden aan Artificiële Intelligentie (AI), algoritmes en datagedreven werken.

Artificiële Intelligentie en algoritmes
Artificiële Intelligentie (AI) en algoritmes staan volop in de aandacht van de politiek en de samenleving. Algoritmes, sets van regels die computers automatisch volgen om problemen op te lossen of vragen te beantwoorden, vormen de kern van veel AI-toepassingen. Bij AI wordt een computer specifiek getraind om taken uit te voeren op basis van patroonherkenning en grote hoeveelheden voorbeelddata. Het gebruik van algoritmes zien we zowel bij private organisaties als bij overheidsorganisaties terug. Variërend van de belastingdienst tot de politie en verschillende gemeenten. De AP heeft in 2023 bijvoorbeeld 5 gemeenten om opheldering gevraagd over het gebruik van een 'fraudescorekaart'. Dit is een algoritme dat risico's op fraude door mensen met een bijstandsuitkering in beeld brengt. Algoritmes kunnen voordelen bieden als het gaat om het analyseren van grote hoeveelheden gegevens en snelle besluitvorming. Ze kunnen ook repetitieve taken automatiseren, waardoor mensen vrijkomen voor meer complexe taken.

De FG houdt intern toezicht op *alle* werkprocessen in de drie gemeenten waar persoons- of politiegegevens in worden gebruikt. Het maakt daarbij niet uit op welke manier dit technisch gezien gebeurt, dus met of zonder algoritmes. In 2023 hebben de drie gemeenten bijvoorbeeld besloten om gebruik te maken van AI, in de vorm van Microsoft Bing/Copilot. Als de drie gemeenten algoritmes gebruiken, moeten ze daarbij aan de eisen uit de AVG en Wpg voldoen. Daarvoor zal eerst moeten worden bepaald *of* en *waar* er verder in de organisaties algoritmes worden ingezet. Dit wordt nu niet standaard vastgelegd of beschreven. Dit betekent dat er mogelijk in de organisaties algoritmes worden gebruikt zonder dat deze vanuit privacy en informatiebeveiliging in beeld zijn. Het advies is om dit overzicht bij de inventarisatiewerkzaamheden in het kader van de verwerkingsregisters in 2024 mee te nemen. Een andere reden om dit overzicht te creëren is de Europese AI-Verordening. Deze gaat vanaf een bepaald moment verplicht stellen dat AI-algoritmes worden gedocumenteerd en in het landelijke Algoritmeregister van de overheid worden opgenomen. Overheden kunnen daar nu al vrijwillig informatie over hun algoritmes publiceren.

Digitale overheid en datagedreven werken
Datagedreven werken biedt gemeenten tal van voordelen, waaronder verbeterde besluitvorming, efficiëntere werkprocessen en beter inzicht in de behoeften van inwoners. Door gegevens te analyseren en te interpreteren, kunnen gemeenten bijvoorbeeld trends in domeinen identificeren en patronen ontdekken. Het gebruik van persoons- en politiegegevens voor datagedreven werken brengt risico's op het gebied van informatiebeveiliging en privacy met zich mee. Het is daarom van belang dat deze onderwerpen in 2024 worden geïntegreerd in elke fase van het dataverwerkingsproces.

4. Conclusie

Informatiebeveiliging en privacy binnen de drie gemeenten is nog in ontwikkeling. De functionarissen op het gebied van informatiebeveiliging en privacy hebben in 2023 een goede basis gelegd om het informatiebeveiliging- en privacymanagement verder in te kunnen richten. Het volwassenheidsniveau binnen de verschillende teams, domeinen en organisaties varieert sterk. Zoals in eerdere verslagen aangegeven is het bewustzijn van proceseigenaren cruciaal om het niveau van informatiebeveiliging en privacy te verhogen. Als zij niet doorhebben dat veranderingen in werkprocessen de bescherming van gegevens beïnvloeden, wordt het moeilijk voor de organisaties om aan de verplichtingen op dit gebied te voldoen.

Jaarlijks stellen de CISO en FG een toezichtverslag op voor de gemeenten over de naleving van de BIO, de AVG en de Wpg. Hieruit volgt een jaarplan van de organisaties voor het opvolgen van de aanbevelingen. Helaas zien de CISO en de FG dat eerdere verbeterpunten de afgelopen jaren maar beperkt zijn opgepakt. Voornamelijk door een gebrek aan capaciteit bij en de noodzaak tot prioritering van informatiebeveiliging en privacy. Het vermogen van de organisaties om aan verbeterpunten te werken wordt inmiddels ook sterk beïnvloed door de werkdruk waar de medewerkers in de teams en de domeinen mee te maken hebben. Hierdoor dreigt het werken aan structurele verbeteringen in het gedrang te komen. Voor 2024 doen de FG en de CISO de volgende aanbevelingen:

Governance

- Verhoog het bewustzijn in de organisaties als het gaat om de rollen bij informatiebeveiliging en privacy (three lines of defense model)
- Verbeter de betrokkenheid van de organisaties bij gemeentebrede acties voor informatieveiligheid en privacy in DOWR-verband
- Bundel (waar mogelijk) adviezen vanuit informatiebeveiliging en privacy aan het management met adviezen uit de andere informatiegebieden
- Maak periodiek sturingsinformatie beschikbaar aan de organisaties en bespreek dit met bestuur en directie
- Bewaak de onafhankelijke positie van derde lijns- functionarissen (CISO en FG)
- Professionaliseer de functie van de CISO en de FG

Privacy en security by design

- Werk achterstanden bij het uitvoeren van risicoanalyses voor privacy (DPIA’s) en informatiebeveiliging (DRA’s) weg en geef prioriteit aan deze werkzaamheden vanuit de teams en domeinen
- Breng de praktijk bij DPIA’s in lijn met de opgestelde procedure
- Zorg voor voldoende kennis en begrip van processen in de organisaties, zodat er gestuurd kan worden op gegevensverwerkingen in informatieketens en werkprocessen
- Zorg dat DPIA’s en DRA’s centraal beschikbaar zijn en bewaak de resultaten

Overzicht creëren

- Werk zo snel mogelijk de drie registers van verwerkingen bij en richt dataclassificatie in
- Besteed aandacht aan de capaciteit in de teams en domeinen bij de actualisatieslag
- Draag zorg voor het bijhouden van de geregistreerde werkprocessen en informatiesystemen

Incidenten

- Deel lessen en ervaringen bij incidenten breed binnen de organisaties
- Dring schaduw IT terug doormiddel van duidelijke afspraken
- Zorg voor een integrale aanpak van informatiebeveiliging en privacy bij de aanschaf van applicaties en diensten

Bewustwording

- Vergroot planmatig het bewustzijn en gebruik verschillende soorten 'bewustwordingsprikkels'

- Dring er bij managers op aan dat zij privacy en informatiebeveiliging als integraal onderdeel van de werkprocessen naar medewerkers uitdragen

Rechten van betrokkenen
- Neem in de privacyverklaringen op hoe gemeenten omgaan met politiegegevens
- Vraag in de organisaties aandacht voor de taken en verantwoordelijkheden bij AVG- of Wpg-verzoeken

Auditverplichting Wet politiegegevens
- Start met verbeterplannen en besteed aandacht aan capaciteit in de teams bij de benodigde acties

Wet beveiliging netwerk- en informatiesystemen (Wbni)
- Besteed aandacht aan de capaciteit bij de inzet van de informatiebeveiligingsfunctionarissen (ISO, TISO en CISO) voor de implementatie van de NIS2-richtlijn (Wbni)

In het privacy- en informatiebeveiligingsplan 2024 staat beschreven wat de drie organisaties concreet zullen doen op het gebied van informatieveiligheid en privacy in 2024.

5. Verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
De AP is de Nederlandse toezichthouder voor de uitvoering van privacywetgeving.

Betrokkene
De persoon waarvan persoonsgegevens of politiegegevens worden verwerkt.

Baseline Informatiebeveiliging Overheid (BIO)
De BIO beschrijft het basisniveau voor informatiebeveiliging binnen de Nederlandse overheid, gebruikt door Rijk, Gemeenten, Waterschappen en Provincies.

Data Protection Impact Assessment (DPIA)
Een instrument om privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

Baselinetoets Basisbeveiligingsniveau (BBN)
Een instrument om informatiebeveiligingsrisico's in kaart te brengen en te bepalen of een proces, informatiesysteem en/of informatie een bepaald Basis beveiligingsniveau (BBN) heeft.

Meldplicht datalekken
Een verplichte melding van datalekken met ernstige gevolgen binnen 72 uur aan de AP.

Persoonsgegevens
Alle informatie die iets zegt over een persoon, zoals naam, adres en geboortedatum.

Politiegegevens
Informatie over mensen die door BOA's wordt gebruikt voor opsporingstaken, zoals gegevens over strafbare feiten.

Rechten van betrokkenen
Onder de AVG en de Wpg hebben mensen rechten, zoals inzage, rectificatie, verwijdering en bezwaar.

Verwerken van persoonsgegevens

Alles wat de gemeente doet met persoonsgegevens of politiegegevens, zoals verzamelen, vastleggen, structureren, opslaan, wijzigen, opvragen of bekijken.

Verwerkingsverantwoordelijke
Een instantie of orgaan dat het doel en de middelen voor de verwerking van persoonsgegevens of politiegegevens vaststelt.

Verwerkingsregister
Een verplicht register waarin de gemeente alle werkprocessen met verwerkingen van persoonsgegevens en politiegegevens bijhoudt, inclusief doeleinden, categorieën persoonsgegevens en bewaartermijnen. Dit moet actueel gehouden worden.