Nota voor Burgemeester en Wethouders

Team: Concernstaf
Onderwerp:
Toezichtjaarverslag informatieveiligheid en privacy 2022

Notagegevens		
Bestuursorgaan	:	B-en-W 9-05-2023
Notanummer	:	2023-247
Datum	:	9-05-2023
Programma	:	11 - Bedrijfsvoering
Portefeuillehouder	:	Burgemeester,
Bijlage(n)	:	Privacy- en informatiebeveiligingsplan 2023.pdf,Toezichtjaarverslag CISO en FG 2022.pdf

Parafering

22-03-2023: Burgemeester
21-03-2023: Regiemanager

Agendering

* 01-05-2023: Gemeentesecretaris/algemeen directeur

Definitieve akkoord

10-05-2023

B & W d.d.: 9-05-2023

Besluit

1. Het toezichtjaarverslag van de Chief Information Security Officer en de Functionaris Gegevensbescherming over 2022 vast te stellen
2. De raadsmededeling vast te stellen en met het toezichtjaarverslag aan te bieden aan de gemeenteraad
3. Kennis te nemen van het privacy- en informatiebeveiligingsplan 2023

De nota en het besluit openbaar te maken.

Inleiding

Gemeenten verwerken op grote schaal informatie en persoonsgegevens van inwoners. Zonder deze gegevens kunnen zij hun taken niet uitvoeren. Het gaat in de praktijk niet alleen om het verwerken van persoonlijke informatie van inwoners, maar ook om de gegevens van medewerkers en relaties van de gemeente. De Baseline Informatiebeveiliging Overheid (BIO) en de Europese Algemene Verordening Gegevensbescherming (AVG) bieden waarborgen voor het beschermen van gegevens. Zij verplichten tot het aantoonbaar treffen van beheersmaatregelen binnen organisaties om informatieveiligheid en privacy te borgen.

De Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) van de gemeente Deventer zien erop toe dat de gemeente bij het verwerken van informatie en persoonsgegevens voldoet aan de verplichtingen uit de BIO en de AVG. De CISO en FG geven hun bevindingen rechtstreeks aan het college van burgemeester en wethouders. Bij dit voorstel treft u het toezichtjaarverslag van de CISO en de FG over het jaar 2022 aan.

De BIO en de AVG zijn omvangrijke en gecompliceerde normenkaders die om structurele inzet vragen van bestuur, management en medewerkers. In het

toezichtjaarverslag komt naar voren dat de structurele inbedding van de informatieveiligheid- en privacygovernance en het risicomanagement bij de gemeente nog volop in ontwikkeling is. Er zijn in 2022 stappen gemaakt in het beheersen van informatieveiligheid- en privacyrisico's teneinde de naleving van de BIO en de AVG in de werkprocessen te borgen. Evenals voorgaande jaren ging het daarbij vooral om het bestendigen van de reeds gehanteerde aanpak. Voor de Wet Politiegegevens (Wpg) stond 2022 vooral in het teken van een nulmeting in de vorm van een externe audit. Uit deze audit is gebleken dat de verwerkingen van politiegegevens binnen de gemeente op veel vlakken nog niet aan de Wpg-eisen voldoen.

Er is in 2022 door de privacyorganisatie aandacht gevraagd voor voldoende capaciteit en middelen bij het uitvoeren van de verplichtingen onder de AVG en Wpg. Dit heeft uiteindelijk voor de budgetten gezorgd die in 2023 tot een capaciteitsuitbreiding bij privacy moeten gaan leiden. Dit betekent wel dat het gebrek aan capaciteit in 2022 op veel AVG-aandachtsgebieden invloed heeft gehad, zoals het actualiseren van het verwerkingsregister, het uitvoeren van risicoanalyses (DPIA's) en op het daadwerkelijk starten met de implementatie van de Wpg.

Aanvullend is ervoor gekozen om u gelijktijdig te informeren over de maatregelen voor 2023 als reactie op de constateringen van de CISO en de FG. Deze zijn te vinden in het privacy- en informatiebeveiligingsplan 2023.

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 BIO en de AVG moeten daarbij in acht worden genomen.

Kader
Algemene Verordening Gegevensbescherming (AVG)
Baseline Informatiebeveiliging Overheid (BIO).

Betrokken partijen en participatie
Niet van toepassing.

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

Financiële consequenties en dekking
Niet van toepassing.

Openbaarmaking en communicatie
Niet van toepassing.

Aanpak en uitvoering
De Privacy Officer en de Information Security Officer gaan samen met de organisatie aan de slag met de in het privacy- en informatiebeveiligingsplan genoemde actiepunten.

gemeente Deventer

RAADSMEDEDELING

Onderwerp	Toezichtjaarverslag informatieveiligheid en privacy 2022		
Nummer	2023-247	**Portefeuillehouder**	Burgemeester,
Team	DEV-CS	**Datum**	9-05-2023

Inleiding
Het college informeert uw raad over het toezichtjaarverslag informatieveiligheid en privacy over het jaar 2022. De Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (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) en de Baseline Informatiebeveiliging Overheid (BIO). De FG en CISO rapporteren hun bevindingen rechtstreeks aan het college van burgemeester en wethouders. Daarnaast informeert het college uw raad over de ENSIA audit 2022.

Kader
Algemene Verordening Gegevensbescherming (AVG)
Baseline Informatiebeveiliging Overheid (BIO).

Kern van de boodschap
Gelet op de aard en de omvang van de gegevensverwerking bij de gemeente Deventer is het van groot belang dat dit zorgvuldig gebeurt. De beginselen van de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO) moeten daarbij in acht worden genomen. Structurele inbedding van de informatieveiligheid- en privacygovernance en het risicomanagement zijn bij gemeente Deventer nog volop in ontwikkeling. Daarnaast legt het college jaarlijks verantwoording af aan de gemeenteraad en aan de verticale toezichthouders (ministeries van BZK, SZW, Financiën) over informatieveiligheid. Hiervoor is in 2017 door de VNG ENSIA ingevoerd: Eenduidige Normatiek Single Information Audit. Dit betekent eenmalige informatieverstrekking en een eenmalige IT-audit.

Nadere toelichting
In het toezichtjaarverslag geven de FG en de CISO een beeld van de stand van zaken bij de gemeente Deventer als het gaat om het naleven van de AVG en de BIO in 2022.

De AVG en de BIO zijn omvangrijke en gecompliceerde normenkaders die om structurele inzet vragen van bestuur, management en medewerkers. In het toezichtjaarverslag komt naar voren dat de structurele inbedding van de informatieveiligheid- en privacygovernance en het risicomanagement bij de gemeente Deventer nog volop in ontwikkeling is. De gemeente heeft in 2022 stappen gezet in het beheersen van informatieveiligheid- en privacyrisico's teneinde de naleving van de BIO en de AVG in de werkprocessen te borgen. Evenals voorgaande jaren ging het daarbij vooral om het bestendigen van de reeds gehanteerde aanpak. Voor de Wet Politiegegevens (Wpg) stond 2022 vooral in het teken van een nulmeting in de vorm van een externe audit. Uit deze audit is

gebleken dat de verwerking van politiegegevens binnen gemeente Deventer op veel vlakken nog niet aan de Wpg-eisen voldoet.

Er is in 2022 door de privacyorganisatie aandacht gevraagd voor voldoende capaciteit en middelen bij het uitvoeren van de verplichtingen onder de AVG en de Wpg. Dit heeft uiteindelijk voor de budgetten gezorgd die in 2023 tot een capaciteitsuitbreiding bij privacy moeten gaan leiden. Dit betekent wel dat het gebrek aan capaciteit in 2022 op veel AVG-aandachtsgebieden invloed heeft gehad, zoals het actualiseren van het verwerkingsregister, het uitvoeren van risicoanalyses (DPIA's) en op het daadwerkelijk starten met de implementatie van de Wpg. Door de capaciteitsuitbreiding is de verwachting dat gemeente Deventer in 2023 op deze aandachtsgebieden zal verbeteren.

Daarnaast informeert het college de gemeenteraad over ENSIA: Eenduidige Normatiek Single Information Audit. ENSIA structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).
Een overzicht van de scores/uitkomsten van de ENSIA audit 2022:
- Deventer is geslaagd voor de verplichte audit DigiD (digitale aansluiting voor onze dienstverlening) en Suwinet (Werk en Inkomen). Op alle normen scoren wij een voldoende.
- Deventer scoort een voldoende voor de uitvoering van de BAG. Echter is er de afgelopen jaren geen luchtfoto signalering en kartering voor de BAG uitgevoerd waardoor de score t.o.v. voorgaande jaar is gedaald. Zonder maatregelen zakken we door de wettelijke ondergrens. Dit is een zorgpunt, waar maatregelen nodig zijn om dit te voorkomen. In 2023 worden daarom de achterstanden van de afgelopen 5 jaar weggewerkt en verwerkt in de BAG. Vanaf 2024 zal het bijhouden van de BAG onderdeel worden van het reguliere beheer.
- Deventer scoort een voldoende op de uitvoering van de BGT. Er is in 2022 door programma Leefomgeving extra geïnvesteerd om de geometrie van de openbare ruimte weer op orde te maken in de BGT.
- Deventer scoort een onvoldoende voor de BRO. Oorzaken hiervoor ligt in het feit dat niet alle bodemonderzoeken worden gepubliceerd op het BRO-loket. De implementatie van de BRO dient verder ingericht te worden in de organisatie. In 2023 worden hier stappen in gezet door een ervaren projectleider aan te trekken om het BRO-loket en vooral de werkprocessen op een goede wijze te implementeren. De dekking hiervoor is al beschikbaar.
- Deventer scoort voldoende op het onderdeel WOZ. Er is oog voor Data integriteit, maandelijks vinden er controles plaats en wordt data geborgd. Uitval van data wordt onmiddellijk opgepakt door de vakgroep WOZ. Daar waar risico's optreden wordt dit gesignaleerd en afgestemd met de leverancier.
- Deventer scoort voldoende op het onderdeel uittreksel Basisregistratie Personen (BRP). Daar waar nodig wordt door de BRP specialist een plan van aanpak opgesteld.
- Deventer scoort voldoende op het onderdeel uittreksel Reisdocumenten. Daar waar nodig wordt door de Reisdocumenten specialist een plan van aanpak opgesteld.

Bijlage:
- Toezichtjaarverslag CISO en FG 2022

Privacy- en informatiebeveiligingsplan

2023

DOWR - Lucas Klekamp - Privacy Officer (PO)

DOWR-i - Wessel Hemels - Information Security Officer (ISO)

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

Voor u ligt het privacy- en informatiebeveiligingsplan voor 2023. In tijden waarin technologie en digitale communicatie een steeds grotere rol spelen in ons dagelijks leven is het belangrijk om te zorgen voor een hoog niveau van informatieveiligheid en bescherming van persoonsgegevens. In dit jaarplan staan we stil bij de uitdagingen voor 2023 en beschrijven we de stappen die we zullen ondernemen om deze uitdagingen aan te gaan. We zijn vastberaden om ons te blijven inzetten voor een veilige en beschermde digitale wereld, waarin de privacy van onze inwoners, partners en medewerkers gewaarborgd is. De bevindingen van de Functionaris Gegevensbescherming (FG) en Chief Information Security Officer (CISO) uit het Toezichtjaarverslag informatieveiligheid en privacy 2022 liggen mede ten grondslag aan de actiepunten in dit plan. De gezamenlijke actiepunten zien zowel op privacy als informatieveiligheid.

In 2022 is er onderzoek gedaan naar de benodigde capaciteitsuitbreiding bij de functies van Privacy Officer (PO), Information Security Officer (ISO) en FG om te kunnen voldoen aan onze verplichtingen onder de Algemene verordening gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg). Dit heeft geleid tot uitbreiding van de capaciteit. Op het moment van schrijven van dit plan (januari 2023) zitten we midden in het wervingsproces voor de functies van PO en ISO. Onduidelijk is nog wanneer nieuwe collega's zullen starten. Daarnaast kunnen we, zeker gezien de huidige arbeidsmarkt, enige onervarenheid verwachten en dus een zekere inwerkperiode. In dit plan hebben we daar waar nodig hiermee rekening gehouden.

Wat willen we in 2023 bereiken?

Het gebruik van persoonsgegevens en andere soorten informatie vindt plaats in (bijna) alle werkprocessen van de gemeenten Deventer, Olst-Wijhe en Raalte. Als overheidsinstelling hebben we een bijzondere verantwoordelijkheid om deze informatie te beschermen. Inwoners zijn immers vaak verplicht om gevoelige gegevens te delen met de gemeente en moeten kunnen vertrouwen op een zorgvuldige omgang met deze gegevens.

Het doel dit jaar is om inzicht te krijgen in deze processen, de verschillende applicaties die hierbij worden gebruikt en de mogelijke risico's die daarbij komen kijken. Dit inzicht verkrijgen gaat om inspanning vragen van de proceseigenaren en van medewerkers die bij de inventarisatie betrokken worden. Door de uitbreiding van de formatie komt er man- of vrouwkracht bij privacy en informatieveiligheid bij waardoor proceseigenaren zo goed mogelijk gefaciliteerd en ondersteund kunnen worden bij het voldoen aan hun verantwoordelijkheden.

Het bereiken van een fase waarbij alle werkprocessen in beeld zijn en beoordeeld zijn op privacy- en informatieveiligheidsrisico's is niet in één jaar te realiseren. Dit zal meerdere jaren duren. In 2023 zal de focus liggen op het neerleggen van het fundament om deze volgende stap in het volwassenheidsniveau van de drie organisatie te kunnen maken.

Financiële consequenties

Per actiepunt is aangegeven of er financiële consequenties bij betrokken zijn. Deze kosten worden gedekt door bestaande informatieveiligheid/ privacy budgetten. Mocht dit voor een bepaald actiepunt niet zo zijn, dan volgt hiervoor een apart voorstel.

Impact organisatie

Dit plan is van toepassing op alle drie de DOWR-gemeenten. Indien een actiepunt een impact heeft op specifiek één of meerdere uitvoerende teams of domeinen wordt dit bij het actiepunt aangegeven. Met impact wordt bedoeld dat het actiepunt naast werkzaamheden voor de PO, ISO, FG of CISO ook werkzaamheden voor de proceseigenaar of andere medewerkers meebrengt.

1. Gezamelijke actiepunten

1.1 Crisisplan

In 2022 zijn grote stappen gezet met het crisisplan. In het tweede kwartaal van 2023 zal de afronding plaatsvinden. Het zal hier met name gaan om het maken van verschillende afspraken tussen de gemeenten. Denk hierbij aan:

- Welke gemeente/burgemeester zal voor de camera komen te staan in geval van een crisis?
- Wat doen we in het geval van ransomware? Wie bepaalt of we betalen en/of wie heeft het stekkermandaat? En wat als er mensenlevens in gevaar komen?

Dit soort scenario's zullen besproken worden tijdens een sessie in april 2023. Vervolgens zullen we het plan oefenen om goed voorbereid te zijn voor als een crisis zich daadwerkelijk voordoet.

Impact Organisatie
Ja, burgemeesters, gemeentesecretarissen en medewerkers openbare orde & veiligheid zijn betrokken bij het afronden van het crisisplan.

Kosten
Ja, gedekt

Planning
Q1 – Q4 2023

1.2 Bewustwording

We willen de kennis van medewerkers op het gebied van informatieveiligheid en privacy verbeteren. Dit doen we aan de hand van een aantal bewustwordingsactiviteiten:

Nanolearning Dit jaar zal weer een nieuwe reeks aan Nanolearning lessen verstuurd worden naar alle medewerkers. Nanolearning bewustwordingscampagnes zijn interactieve en informatieve e-learnings die niet langer dan een paar minuten duren. Hierdoor zijn ze gemakkelijk in te passen in de dagelijkse werkzaamheden van medewerkers. Gezien de dalende deelnamepercentages van afgelopen jaar zullen managers opnieuw gevraagd worden het belang van Nanolearning richting hun team of domein uit te dragen. Daarnaast zal er ook op andere manieren aandacht worden gevraagd voor Nanolearning, zoals het uitdelen van een wisselbeker aan het best deelnemende team of domein.

Onboarding Voor nieuwe medewerkers zal er een animatiefilmpje gemaakt worden waarin op een ludieke wijze wordt toegelicht wat het belang van privacy en informatieveiligheid is en wat er als medewerker op dit gebied van je wordt verwacht. Dit filmpje wordt onderdeel

van de onboarding/introductie programma's van de drie gemeenten.

Bewustwording proceseigenaren Het actualiseren van de verwerkingsregisters en het op grotere schaal uitvoeren van risicoanalyses, zoals beschreven staat in onderstaande actiepunten, gaat om een inspanning vragen van proceseigenaren. Om ze hun verantwoordelijkheden te kunnen laten nemen en te voorzien in hun informatiebehoefte, zal er bij de verschillende overleggen van team/domeinmanagers worden toegelicht wat er van hen wordt gevraagd.

Sharepointpagina Er zal een Sharepointpagina worden gemaakt waarop allerlei informatie, zoals beleid of werkinstructies, beschikbaar komt voor alle medewerkers. Zie het als een soort kennisbank voor privacy en informatieveiligheid.

Impact Organisatie
Ja, alle medewerkers wordt gevraagd om deel te nemen aan het Nanolearningprogramma. Daarnaast zullen nieuwe medewerkers bij de onboarding deelnemen aan het introductieprogramma.

Kosten
Ja, gedekt

Planning
Q1 – Q4 2023

1.3 Uitwerken werkwijze vastlegging verwerkingsregisters en risicoanalyses

De Sharepointpagina 'Informatieveiligheid en Privacy Centraal' wordt gebruikt om de verantwoordingsdocumentatie omtrent privacy en informatieveiligheid vast te leggen. Deze werkomgeving zal verder ingericht worden om de verwerkingsregisters, risicoanalyses en de resultaten daarvan op een overzichtelijke manier vast te kunnen leggen. Het gaat hier om een andere Sharepointomgeving dan de hierboven genoemde kennisbank.

Voor informatieveiligheid wordt er naast Sharepoint ook gebruik gemaakt van de risicomanagementtool Naris.

Impact Organisatie
Nee

Kosten
Nee

Planning
Q2 2023

1.4 Uitvoeren risicoanalyses privacy en informatieveiligheid op bestaande werkprocessen

Zoals is gebleken uit het onderzoek naar capaciteitsuitbreiding en ook te lezen is in het toezichtjaarverslag van de FG en de CISO, zijn er nog veel bestaande werkprocessen binnen de drie gemeenten waar nog geen DPIA en Baselinetoets op zijn uitgevoerd.

Dit jaar zal er een werkwijze worden ontwikkeld om deze achterstand weg te werken. Ook zal hierbij worden onderzocht wat dit van de teams en domeinen qua uren gaat vragen. Dit is afhankelijk van hoeveel werkprocessen als 'hoog risico verwerking' worden gezien en kan dus per team/domein erg verschillen. Met de betreffende proceseigenaren zal worden onderzocht of er eventuele knelpunten in capaciteit aan de kant van de teams/domeinen zijn, zodat dit meegenomen kan worden in de prioritering vanaf 2024.

Aan het eind van 2023 zullen de eerste risicoanalyses op bestaande werkprocessen worden uitgevoerd.

Impact Organisatie
Ja, proceseigenaren en door de proceseigenaar aangewezen medewerkers worden betrokken bij het uitvoeren van risicoanalyses.

Kosten
Nee

Planning
Q3-Q4 2023

2. Actiepunten privacy

2.1 Actualiseren verwerkingsregisters

Gemeenten zijn verplicht een register bij te houden waarin alle structurele verwerkingen van persoonsgegevens zijn opgenomen. Hiermee wordt inzicht verkregen in de stromen en opslag van persoonsgegevens. Sinds 2018 zijn de registers van de drie DOWR-gemeenten niet meer geactualiseerd. Proceseigenaren zijn ervoor verantwoordelijk dat hun processen volledig en actueel in het register zijn opgenomen. De PO is verantwoordelijk voor het coördineren van de actualisatie en het beheer van de registers.
Naast de structurele uitbreiding van de formatie zal er tijdelijk extra versterking komen om de registers te actualiseren. Er wordt nog onderzocht of er iemand tijdelijk in dienst wordt genomen of dat er externe inhuur wordt ingezet.

Vanuit privacy en informatieveiligheid zijn we in gesprek met de collega's van informatiebeheer over de verwerkingsregisters. Dit omdat zij vanuit archiveringsperspectief ook een inventarisatie van processen moeten uitvoeren. Om ervoor te zorgen dat werkzaamheden niet dubbel worden gedaan en om te voorkomen dat proceseigenaren niet meerdere malen dezelfde vragen worden gesteld, houden we elkaar op de hoogte van wat we aan het doen zijn. Waar de werkvelden van privacy, informatieveiligheid en informatiebeheer elkaar overlappen zal informatie worden hergebruikt.

Impact Organisatie
Ja, proceseigenaren en door hen aangewezen medewerkers worden om input gevraagd bij het actualiseren van de verwerkingsregisters. Hoeveel uren dit kost is afhankelijk van het aantal processen binnen een team of domein.

Kosten
Ja, gedekt

Planning
Q2 - Q4 2023

2.2 Actualiseren algemeen privacybeleid

De colleges van B&W van de drie DOWR-gemeenten hebben in 2018 algemeen privacybeleid vastgesteld waarin ze hun visie op gegevensbescherming hebben verwoord. Hierin is onder andere beschreven hoe de verantwoordelijkheden op strategisch en operationeel niveau zijn geborgd.

Sinds 2018 hebben de gemeenten ervaring opgedaan met het uitvoeren van het beleid en zijn er de nodige ontwikkelingen geweest, waaronder de komst van de Wpg. Dit maakt dat het privacybeleid geëvalueerd en geactualiseerd moet worden en opnieuw wordt voorgelegd aan de drie colleges ter vaststelling.

Impact Organisatie
Nee

Kosten
Nee

Planning
Q3 2023

2.3 Uitwerken werkwijze doorbelasting uren DPIA

Naar aanleiding van het onderzoek naar de benodigde capaciteitsuitbreiding hebben de drie gemeenten besloten dat een deel van de kosten gedekt moet worden uit projecten. Dit geldt voor nieuwe of gewijzigde verwerkingen van persoonsgegevens waarbij een DPIA moet worden uitgevoerd. De uren die de PO, ISO en FG besteden aan een DPIA dienen te worden doorbelast aan het team of domein waar de DPIA op ziet. Hiervoor zal een werkwijze worden ontwikkeld, waar-

bij zoveel mogelijk zal worden aangesloten bij soortgelijke bestaande constructies binnen DOWR-i.

Impact Organisatie
Nee

Kosten
Nee

Planning
Q1 2023

2.4 Inrichten auditproces Wet Politiegegevens

De teams en domeinen waarbinnen BOA's werkzaam zijn dienen op grond van de Wpg elk jaar een interne privacy audit uit te voeren en elke vier jaar een externe audit. Er zal een auditproces ontwikkeld worden waarbij onder andere afspraken worden gemaakt over wie welke rol heeft en hoe de kosten voor de externe auditor worden verdeeld.

Impact Organisatie
Ja, de betreffende proceseigenaren worden betrokken bij het inrichten van het auditproces

Kosten
Ja, voorstel

Planning
Q2 2023

3. Informatiebeveiliging actiepunten

3.1 Beveiliging van mobiele apparaten

HHet beveiligen van mobiele apparaten, zoals smartphones, tablets en laptops, heeft als doel om de vertrouwelijke informatie op deze apparaten te beschermen tegen onbevoegde toegang, verlies of diefstal. Dit omvat zowel de gegevens op het apparaat zelf als de informatie die via het apparaat wordt verzonden of ontvangen.

Het beveiligen van mobiele apparaten is belangrijk omdat deze apparaten voornamelijk worden gebruikt voor werkgerelateerde doeleinden en dus vaak vertrouwelijke informatie bevatten. Denk daarbij aan vertrouwelijke bedrijfsinformatie, persoonlijke identificatie- en financiële gegevens en gezondheidsgegevens.

Zodra de mobiele apparaten voldoen aan de beveiligingstandaard krijgen medewerkers de mogelijkheid om informatie lokaal op de laptop te kunnen verwerken (met bijvoorbeeld Word en Excel). Op termijn willen we ernaar toe werken dat ook vakapplicaties en ons zaaksysteem buiten VDI toegankelijk zijn. Op het moment van schrijven is dat helaas nog niet mogelijk.

Impact Organisatie
Nee

Kosten
Ja, gedekt

Planning
Q2 2023

3.2 Monitoring en controle

Het doel van monitoring vanuit informatieveiligheid is om de integriteit, beschikbaarheid en vertrouwelijkheid van informatiesystemen en gegevens te waarborgen. Dit wordt ook wel SIEM SOC genoemd (Security Information & Event Management Monitoring en Security Operations Center) maakt het mogelijk om de digitale gezondheid van de systemen te volgen en om tijdig te reageren op bedreigingen en incidenten.

In 2023 nemen wij afscheid van onze huidige monitoringsdienstverlening en zal deze vervangen worden door een nieuwe leverancier.

Impact Organisatie
Nee

Kosten
Ja, gedekt

Planning
Q2 2023

3.4 Voorbereiding NIS2

De NIS2 (Network and Information Security Directive) is een Europese richtlijn die de informatieveiligheid van digitale systemen regelt en beschermt. Het is onderdeel van de digitale markt binnen de Europese Unie en heeft als doel om de digitale economie en de digitale samenleving veiliger te maken.

Met de komst van NIS2 wordt het voor bedrijven verplicht om hun digitale systemen op een bepaalde manier te beveiligen en te waarborgen dat ze beschermd zijn tegen digitale dreigingen.

Gemeenten zullen hier ook aan moeten gaan voldoen. Het lijkt erop dat dit in 2025 verplicht zal worden. Daarom zal er in 2023 onderzoek gedaan worden naar de impact van deze Europese richtlijn. Dit om een reële inschatting te kunnen maken van de verwachte toename in kosten en inspanningen.

Impact Organisatie
Nee

Kosten
Nee

Planning
Q4 2023

3.4 Actualisatie Informatiebeveiligingsbeleid

De BIO 2.0 (Baseline Informatiebeveiliging Overheid 2.0) is de vernieuwde versie van de informatiebeveiligingsnorm. Het DOWR informatiebeveiligingsbeleid zal in 2023 geactualiseerd worden en in lijn worden gebracht met de nieuwe versie van de BIO.

Impact Organisatie
Nee

Kosten
Nee

Planning
Q4 2023

3.5 Netwerk- en Firewallmigratie

In 2022 is de netwerkmigratie naar de nieuwe netwerkarchitectuur voor het grootste deel afgerond. De voordelen van de nieuwe architectuur (vanuit informatieveiligheid) zijn onder andere segmentatie, authenticatie, redundantie en verlaagde beheerslast. In 2023 zullen de laatste actiepunten op dit vlak worden uitgevoerd.

Voor de firewallmigratie sluiten we een firewall met hogere snelheid aan op het nieuwe netwerk, zodat we in de toekomst kunnen doorgroeien naar hogere (internet)snelheden. De hoeveelheid data die we als organisatie verwerken neemt toe, we werken meer vanuit huis en we werken meer in de cloud. Dit alles maakt het nodig om hierin te investeren om efficiënt en snel genoeg de verwachte toename van data te kunnen verwerken.

Impact Organisatie
Nee

Kosten
Ja, gedekt

Planning
Q2 2023

TOEZICHTJAARVERSLAG

INFORMATIEVEILIGHEID EN PRIVACY 2022

Colleges van burgemeester en wethouders
Gemeentes Deventer, Olst-Wijhe en Raalte
Wessel Hemels, Chief Information Security Officer
Lotte Schieving, Functionaris Gegevensbescherming
Maart 2023

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

Inhoud

Inleiding en samenvatting 3
Aandachtsgebieden 4
Governance 4
Risicoanalyses 5
Overzicht creëren 6
Incidenten 7
Bewustwording 8
Rechten van betrokkenen 9
Klachten 9
Security en privacy by design 10
Ontwikkelingen 10
Wet politiegegevens 10
Dreigingsbeeld 2023-2024 10
BIO 2.0 / NIS2 11
Crisisplan Cybersecurity 11
Rekenkameronderzoek 12
Conclusie 12
Verklarende woordenlijst 13

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

Inleiding en samenvatting

Gemeenten verwerken op grote schaal informatie en persoonsgegevens van inwoners. Zonder deze gegevens kunnen zij hun taken niet uitvoeren. Het gaat in de praktijk niet alleen om het verwerken van persoonlijke informatie van inwoners, maar ook om de gegevens van medewerkers en relaties van de gemeente. De Baseline Informatiebeveiliging Overheid (BIO) en Europese Algemene Verordening Gegevensbescherming (AVG) bieden waarborgen voor het beschermen van gegevens. Zij verplichten tot het aantoonbaar treffen van beheersmaatregelen binnen organisaties om informatieveiligheid en privacy te borgen. Het onjuist en onzorgvuldig gebruik van gegevens kan grote gevolgen hebben voor mensen en kan het vertrouwen van inwoners in de gemeente en haar bestuurders schaden. Incidenten waarbij persoonsgegevens kunnen vrijkomen, gewijzigd worden of worden vernietigd kunnen daarnaast een grote impact hebben op medewerkers van de getroffen gemeente. De organisatie is soms maanden bezig met de nasleep van een incident. Onvoldoende naleving van de AVG kan verder leiden tot forse boetes van de Autoriteit Persoonsgegevens (AP) en schadeclaims van gedupeerde betrokkenen.

In dit toezichtjaarverslag geven de Chief Information Security Officer (CISO) en de Functionaris voor gegevensbescherming (FG) een beeld van de stand van zaken bij de gemeenten Deventer, Olst-Wijhe en Raalte als het gaat om het naleven van de BIO en de AVG in 2022. Dit doen zij in hun rol van onafhankelijke toezichthouders.

De uitvoering van de BIO en de AVG heeft een blijvende grote invloed op bijna alle werkprocessen van gemeenten. Gemeenten moeten werkprocessen waarin informatie en persoonsgegevens worden verwerkt inrichten volgens de uitgangspunten van de BIO en de AVG. Het jaar 2022 stond, evenals voorgaande jaren, vooral in het teken van het bestendigen van de informatieveiligheid- en privacy aanpak. De drie organisaties hebben daarbij stappen gezet in reeds gestarte verbeterplannen en activiteiten ondernomen gericht op de verdere inbedding van het risicomanagement. Bijvoorbeeld het uitvoeren van Data Protection Impact Assessments (DPIA's) en baselinetoets Basis Beveiligings Niveau (BBN). In 2022 is duidelijk geworden dat voor het verwerken van politiegegevens, die onder de Wet politiegegevens (Wpg) vallen, een ander en strenger regime dient te gelden dan voor persoonsgegevens. Voor de Wpg stond 2022 in het teken van een nulmeting in de vorm van een externe audit. Uit deze audit is gebleken dat de verwerkingen van politiegegevens binnen de drie gemeenten op veel vlakken nog niet aan de Wpg-eisen voldoen. De verwerkingen van politiegegevens zijn bijvoorbeeld nog niet opgenomen in de registers van verwerkingen, er is nog geen FG aangewezen voor het toezicht op de Wpg en er zijn nog geen wettelijk verplichte DPIA's uitgevoerd. De gemeenten Deventer, Olst-Wijhe en Raalte hebben in 2022 in beeld gebracht wat de verplichtingen onder de AVG en de Wpg daadwerkelijk met zich meebrengen qua werkzaamheden en de inzet van de Privacy Officer (PO), de FG en de Information Security Officer (ISO). De resultaten van dit onderzoek hebben uiteindelijk voor de budgetten gezorgd die in 2023 tot een capaciteitsuitbreiding bij privacy moeten gaan leiden. Dit betekent wel dat het gebrek aan capaciteit bij privacy in 2022 op veel AVG-aandachtsgebieden invloed gehad, zoals het actualiseren van het verwerkingsregister en het uitvoeren van DPIA's, en op het daadwerkelijk starten met de implementatie van de Wpg.

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

In dit toezichtjaarverslag brengen de CISO en de FG verslag uit aan de colleges van burgemeester en wethouders van de gemeenten Deventer, Olst-Wijhe en Raalte als het gaat om de naleving van de BIO en de AVG bij gegevensverwerkingen die onder de verantwoordelijkheid van deze colleges worden uitgevoerd. Het rapport vangt aan met de bevindingen van de CISO en de FG bij de verschillende onderdelen van de BIO en de AVG. De CISO en de FG geven per aandachtsgebied aan wat de aanbevelingen zijn voor 2023. Deze zien er als volgt uit:

1. **Governance** Verbeter het eigenaarschap over privacy en informatieveiligheid bij het management
2. **Risicoanalyses** Voer DPIA's en Baselinetoetsen uit en registreer de resultaten
3. **Overzicht creëren** Actualiseer de drie registers van verwerkingen en pas dataclassificatie toe
4. **Bewustwording / Rechten van betrokkenen** Vergroot doormiddel van inwerkprogramma's en materie specifieke trainingen planmatig het bewustzijn

Vervolgens gaan de CISO en de FG in op ontwikkelingen die in 2023 extra aandacht vragen van de drie organisaties. Het toezichtjaarverslag sluit af met een conclusie.

Aandachtsgebieden

Governance

De PO adviseert de gemeenten Deventer, Olst-Wijhe en Raalte over de naleving van de privacywetgeving en fungeert als eerste aanspreekpunt voor de drie gemeentelijke organisaties. De FG is verantwoordelijk voor het toezicht op de naleving van de privacywetgeving. De ISO adviseert de drie gemeenten over de naleving van de BIO en vervult een met de PO vergelijkbare adviserende rol daar waar de privacywerkzaamheden informatieveiligheid raken. De CISO is verantwoordelijk voor het toezicht op de naleving van de BIO.

In 2022 is het Privacy en Informatieveiligheid Toezichtsorgaan DOWR (PIT DOWR) periodiek bij elkaar gekomen om de aanpak van informatieveiligheid en privacy te bespreken. Daarin namen in ieder geval de Chief Information Officers (CIO's), de FG, de PO, de CISO en de ISO plaats. Uit deze overleggen kwam opnieuw naar voren dat de managers van de individuele gemeenten zich slecht aangesloten voelen bij de uitvoering van de aanpak bij informatieveiligheid en privacy door de voornamelijk in DOWR-verband opererende functionarissen. Het gebrek aan aansluiting op besluitvormend niveau zorgt er onder andere voor dat managers zich minder bewust zijn van hun verantwoordelijkheden bij deze aanpak. Het verdient aanbeveling in 2023 de managers van de drie gemeenten te betrekken bij het verbeteren van deze situatie.

De PO, FG en ISO hebben in 2021 een discrepantie geconstateerd tussen het aantal uren dat zij op dat moment ter beschikking hadden voor de uitvoering van de privacywerkzaamheden voor de drie gemeenten en het aantal uren dat zij feitelijk nodig hadden. Hierdoor konden de gemeenten Deventer, Olst-Wijhe en Raalte niet voldoen aan hun verplichtingen onder de AVG op het gebied van het verwerkingsregister, de DPIA's en de bewustwordingsactiviteiten en niet voldoen aan hun verplichtingen onder de Wpg. De FG en PO hebben daarom in 2022 onderzoek gedaan naar de benodigde capaciteitsuitbreiding bij privacy en inzichtelijk gemaakt wat de werkzaamheden van de

PO, FG en ISO met zich meebrengen. Zij concludeerden dat het uitvoeren van de privacywerkzaamheden onder de AVG en de Wpg tot een uitbreiding van 2 FTE PO, 0,4 FTE FG en 1,6 FTE ISO zou moeten leiden. De drie gemeenten hebben de daartoe benodigde budgetten opgenomen in de begroting voor 2023. In het kwartaaloverleg PIT DOWR van 24 november 2022 is door de drie gemeenten besloten om 2 FTE PO en 1,3 FTE ISO te gaan werven boven op de bestaande formatie. De gemeente Raalte heeft ervoor gekozen voor wat betreft de ISO en de PO een uitzondering te maken en slechts de helft van het benodigde budget op te nemen. De reden hiervoor is dat de organisatie gefaseerd te werk wil gaan. Het advies is om het resterende bedrag in Raalte alsnog mee te nemen in de begroting voor 2024.

Risicoanalyses

DPIA's

Op grond van de AVG zijn gemeenten verplicht om DPIA's uit te voeren voor verwerkingen van persoonsgegevens met een hoog risico. Daarvan is bijvoorbeeld sprake wanneer een gemeente op grote schaal bijzondere persoonsgegevens gaat verwerken. Voorafgaand aan de verwerking moet er dan een beoordeling worden uitgevoerd van de effecten van de beoogde activiteiten op de bescherming van persoonsgegevens. Ook moet in kaart worden gebracht hoe bepaalde privacyrisico's kunnen worden ondervangen. Het doel is om privacy op deze manier onderdeel te laten zijn van de belangenafweging rondom gegevensverwerkingen. Na het doorlopen van de DPIA dient het advies van de FG te worden ingewonnen. In 2022 heeft de AP het belang van DPIA's nogmaals onderstreept door aan de korpschef in Rotterdam een boete van € 50.000 euro op te leggen voor het ten onrechte niet uitvoeren van een DPIA voorafgaand aan het gebruik van camera-auto's. Personen werden daarbij herkenbaar in beeld gebracht om groepsvorming tegen te gaan.

In het onderzoek van de FG en PO naar de benodigde capaciteitsuitbreiding bij privacy in de drie gemeenten kwam naar voren dat er in 2022 nog steeds een omvangrijk aantal DPIA's uitgevoerd moest worden. Specifiek ging het om in totaal 107 DPIA's op zowel bestaande alsnog te starten verwerkingen (48 in de gemeente Deventer, 27 in de gemeente Olst-Wijhe en 32 in de gemeente Raalte). In 2022 zijn er in totaal 6 pre-DPIA's ingevuld en 2 DPIA's afgerond (allebei in de gemeente Deventer). Bij één van deze DPIA's zijn middelen ter beschikking gesteld om de DPIA gedeeltelijk door een externe uit te laten voeren. Gedurende het jaar zijn er opnieuw nieuwe en gewijzigde verwerkingen aangemeld bij de PO. De DPIA-werkachterstand in DOWR-verband is daarmee ongeveer gelijk gebleven ten opzichte van 2021.

Het onderzoek van de FG en PO in 2022 heeft inzichtelijk gemaakt wat de werkzaamheden van de PO, FG en ISO met zich meebrengen als het gaat om het uitvoeren van DPIA's. Elke DPIA brengt, afhankelijk van het soort werkproces en gebruikte applicatie(s), een andere werkdruk met zich mee. Een factor vormt bijvoorbeeld de grootte en complexiteit van de gegevensverwerking. Er is in kaart gebracht dat de PO, FG en ISO respectievelijk gemiddeld 36, 12 en 26 uur aan één DPIA dienen te besteden. Het uitbreiden van de formatie heeft tot gevolg dat er in 2023 bij nieuwe of gewijzigde verwerkingen van persoonsgegevens rekening gehouden zal moet worden met het doorbelasten van deze werkzaamheden. Het advies is om daarbij aandacht te besteden aan het eventueel wijzigen van reeds beschikbare projectbudgetten en goedgekeurde Verkorte initiatie documenten (VID's).

Het onderzoek van de FG en PO naar de benodigde capaciteitsuitbreiding heeft niet alleen inzichtelijk gemaakt wat de DPIA-werkzaamheden voor de PO, FG en ISO meebrengen, maar ook welke uren de

proceseigenaar (of een aangewezen medewerker) aan één DPIA in diens team of domein dient te besteden. Het verdient aanbeveling in 2023 in de teams en domeinen uren vrij te maken voor het uitvoeren van risicoassessments en het implementeren van beheersmaatregelen. Het gaat om 13 uur per DPIA. Het is aan te raden proceseigenaren op tijd te betrekken bij het uitvoeren van DPIA's, zodat zij keuzes kunnen maken over het plannen en prioriteren van de benodigde werkzaamheden.

Het uitvoeren van DPIA's resulteert in veel documentatie. In 2022 is aandacht besteed aan het aantoonbaar vastleggen van de bevindingen en resultaten op de SharePoint genaamd Informatieveiligheid en Privacy Centraal. Per gemeente bevat deze SharePoint inmiddels een, hetzij verouderd, verwerkingsregister waarbij per verwerking in een bibliotheek ingevulde vragenlijsten, rapportages en adviezen van de FG kunnen worden gedocumenteerd. Naast het voorbereiden van de organisaties is ook het verder uitwerken van de vastlegging van de resultaten van assessments een belangrijke succesfactor bij het wegwerken van de DPIA-werkachterstand. Het advies is om met de nieuwe privacybezetting een werkwijze te ontwikkelen die ervoor zorgt dat veranderingen in de AVG-compliance ten gevolge van adviezen en risicoassessments overzichtelijk kunnen worden geregistreerd. Daarbij moet aandacht worden besteed aan de planning van DPIA's, het verifieerbaar en vindbaar blijven van de DPIA-resultaten, het monitoren van de voortgang als het gaat om de opvolging van beheersmaatregelen en het eventueel hergebruiken van kennis over de in kaart gebrachte werkprocessen.

Baselinetoetsen BBN
Op grond van de BIO zijn gemeenten verplicht om Baselinetoetsen uit te voeren op informatiestromen binnen de gemeente. Denk hierbij aan systemen, processen of ander soortgelijke bronnen. In 2022 zijn enkele processen samen met privacy doormiddel van DPIA's in kaart gebracht. Voor het verkrijgen van een volledig overzicht van de verschillende soorten informatie binnen de drie gemeenten wordt geadviseerd om bij het uitvoeren van DPIA's in 2023 gelijktijdig de informatie op te halen die noodzakelijk is voor de Baselinetoetsen.

Voor informatieveiligheid is het daarnaast van belang om ook analyses uit te voeren op processen waar geen persoonsgegevens in worden verwerkt, maar waar de vertrouwelijkheid, beschikbaarheid en integriteit van informatie wel geanalyseerd moet worden. Denk hierbij aan financiële gegevens of kritische processen. Het advies is om in 2023 als gemeenten een werkwijze te ontwikkelen voor het structureel uitvoeren van de verplichte Baselinetoetsen.

Overzicht creëren

Register van verwerkingen
Gemeenten moeten kunnen aantonen dat zij handelen in overeenstemming met de AVG. Dat betekent dat zij onder andere een register van verwerkingsactiviteiten dienen bij te houden. Het doel van dit register is inzicht hebben in de structurele verwerkingen van persoonsgegevens en de stromen van persoonsgegevens binnen de organisatie.

Alle drie de gemeenten hebben hun verwerkingen van persoonsgegevens in 2018 in een register van verwerkingsactiviteiten opgenomen. Bij veel van de opgenomen verwerkingen kan niet meer worden ingestaan voor de juistheid en volledigheid van de verwerkingen. Er stond een actualisatie van de registers gepland voor 2022. Managers zou gevraagd worden om de verwerkingen in het register die onder hun verantwoordelijkheid vallen na te gaan en daarbij aan te geven of zij nog up-to-date waren.

Ondanks dat er een begin is gemaakt met het betrekken van de managers bij deze plannen, heeft de daadwerkelijke actualisatie nog niet plaatsgevonden vanwege een gebrek aan capaciteit bij privacy. De PO dient de actualisatie van de registers namelijk te coördineren.

Gezien de grootte van de actualisatieslag is het aan te raden om hier in 2023 een externe partij voor in te schakelen. Aangezien de juistheid en volledigheid van het register daarna periodiek bijgehouden dient te worden, zal daarnaast een proces moeten worden ontwikkeld voor het tijdig nalopen van wijzigingen in de registers van verwerkingen van de drie gemeenten. Dit om achterstanden of vervuiling in de geregistreerde structurele verwerkingen zoveel mogelijk te voorkomen.

Dataclassificatie
Het belang van informatie classificeren is inzicht krijgen in de waarde van informatie over de assen Beschikbaarheid, Integriteit en Vertrouwelijkheid. Het aspect persoonsgegevens valt daarbij onder de as vertrouwelijkheid. De andere assen zijn onder andere van belang voor bedrijfscontinuïteit (beschikbaarheid) en de vereiste kwaliteit van de gegevens (integriteit).

Als er inzicht is in de waarde van informatie binnen de gemeenten kunnen de organisaties passende maatregelen nemen om deze informatie te beschermen. In 2022 zijn er enkele stappen gezet op het vlak van dataclassificatie. De drie gemeenten hebben ervoor gekozen alle informatie te classificeren als BBN2, Basis Beveiligingsniveau 2, tenzij anders wordt aangetoond. BBN2 is van toepassing op het moment dat er vertrouwelijke informatie wordt verwerkt, mogelijke incidenten kunnen leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en de veiligheid van andere systemen afhankelijk is van de veiligheid van het systeem.

Het advies is om in 2023 een werkwijze te ontwikkelen voor het structureel classificeren van informatie. Het verdient aanbeveling om dit een plek te geven in de diepgaande risicoanalyses aangezien daarbij de informatie in de gemeenten reeds wordt geanalyseerd.

Incidenten

Beveiligingsincidenten
In 2022 zagen we bij de drie gemeenten een toename van misbruik door middel van phishing. Waar phishing door criminelen wordt gebruikt om (gevoelige) informatie te verzamelen of accounts over te nemen, zien we specifiek een toename op zogenoemde *Spear Phishing* (een gerichte aanval op een persoon of organisatie). Hierbij wordt gebruik gemaakt van een vertrouwde bron (maar met een vals e-mailadres), bijvoorbeeld daar waar een e-mail wordt verstuurd door een burgemeester of een financieel manager. Deze e-mail wordt vervolgens naar een select aantal mensen gestuurd, bijvoorbeeld naar raadsleden of naar financieel medewerkers. In dit soort e-mails wordt vaak een verzoek gedaan om geld of specifieke informatie. Een belangrijk onderdeel is de nadruk op urgentie. De verzender geeft aan dat deze zich in een benarde situatie bevindt en snel het geld of de informatie moet hebben.

In 2022 zagen we bij de drie gemeenten ook een toename van e-mail aanvallen via derden, vertrouwde, partijen. Hier is het doel van de crimineel om zoveel mogelijk accounts te verzamelen en deze in de toekomst in te zetten voor andere (kwaadaardige) doelen of om nog meer accounts te verzamelen.

Bij beide soorten aanvallen blijft het in 2023 van belang om kritisch om te gaan met e-mails en bij twijfel de afzender telefonisch te verifiëren. Verder is het van belang dat dit soort voorvallen worden gemeld bij de Servicedesk.

Datalekken
Bij datalekken gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens zonder dat dit de bedoeling is. Van de datalekken die zich in 2022 in de drie gemeenten voordeden vielen de meeste opnieuw in de categorie ‘persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger’. Het betreft vaak een verkeerde adressering van e-mail of post. Dit kan vervelende gevolgen hebben voor de betrokkene, zeker als het gaat om gevoelige informatie of kwetsbare personen. Om die reden blijft het van belang dat medewerkers in 2023 op de risico’s bij het versturen van persoonsgegevens worden gewezen en goed worden geïnstrueerd. Voor zover datalekken intern gemeld en geregistreerd zijn, gaat het slechts in enkele gevallen om incidenten die ernstige nadelige gevolgen hebben gehad voor inwoners.

Bewustwording

Bewustzijn op het gebied van informatieveiligheid en privacy vraagt om voortdurende aandacht en zorg. In 2022 hebben de ISO en PO doormiddel van eenmalige acties bij verschillende teams en domeinen in de drie gemeenten aandacht gevraagd voor hoe medewerkers om moeten gaan met de informatie en persoonsgegevens waar zij dagelijks mee werken. Ook is het bewustzijn op het gebied van informatieveiligheid en privacy in de organisaties bevordert door gebruik te maken van NanoLearning. Alle medewerkers van Deventer, Olst-Wijhe en Raalte kregen om de drie weken een minicursus van 1-3 minuten toegestuurd waarbij ze door middel van een stukje tekst of een korte opdracht iets leerden over informatieveiligheid en privacy. Bij de evaluatie gaven medewerkers aan dat de inhoud van de lessen hun kennis van informatieveiligheid en privacy had vergroot, maar was ook te zien dat de deelnamepercentages inmiddels waren gezakt van gemiddeld 60% naar 40%. De drie gemeenten hebben besloten om in 2023 door te gaan met de toepassing van NanoLearning. Het verdient aanbeveling managers daarbij opnieuw voor te lichten over het belang van deelname en ze te vragen dit richting hun medewerkers uit te dragen. Dit om de groei in de bewustwording rondom de thema’s te behouden.

Eén van de redenen voor het uitbreiden van de capaciteit bij privacy in 2022 was het gebrek aan ruimte voor structurele aandacht voor het inwerken van medewerkers en voor specifieke onderwerpen, zoals dossiervorming in het sociaal domein. Het advies is om in 2023 ook op deze manieren planmatig het bewustzijn in de drie organisaties te verhogen en te verstevigen. Privacy en informatieveiligheid zouden een vast onderdeel moeten worden van het functioneren van medewerkers. Waar informatieveiligheid bijvoorbeeld in eerdere jaren meer werd ervaren als een 'ICT-feestje’ zal het onderwerp een onderdeel moeten worden van ieder zijn of haar professie.

Rechten van betrokkenen

De AVG kent een betrokkene verschillende privacyrechten toe. Deze rechten kunnen zij alleen doen gelden op hun eigen persoonsgegevens. Zo kunnen zij bijvoorbeeld het recht om inzage gebruiken om inzicht te krijgen in de verwerking van zijn of haar persoonsgegevens bij een gemeente. Betrokkenen worden door middel van de privacyverklaring op de website van de gemeenten geïnformeerd over zijn of haar privacyrechten. Ook wordt hierin aangegeven op welke wijze verzoeken bij de gemeenten kunnen worden ingediend. In 2022 werden er in Deventer 4 aanvragen, in Olst-Wijhe 2 aanvragen en in Raalte 1 aanvraag ingediend in het kader van 'rechten van betrokkenen'. Bij de betreffende teams en domeinen werden betrokkenen proactief door medewerkers van de gemeenten ondersteund bij het indienen en laten behandelen van het AVG-verzoek.

De AVG schrijft voor dat de gemeente per ommegaande, doch uiterlijk binnen één maand, reageert op een betrokkene die een beroep doet op privacyrechten. Het besluit op een dergelijk verzoek kan slechts in complexe gevallen met twee maanden worden verdaagd. Van de AVG-verzoeken in 2022 werden er 2 verzoeken (1 verzoek in Olst-Wijhe en 1 verzoek in Raalte) niet tijdig afgehandeld. De inbedding van de procedure bij het behandelen van AVG-verzoeken bleek bij deze gevallen niet toereikend om de verzoeken binnen de gestelde termijn af te kunnen handelen. De medewerkers van de drie gemeenten die aan de behandeling van een AVG-verzoek hebben meegewerkt hebben inmiddels ervaring met het herkennen van verzoeken en met wat zij moeten doen op het moment waarop zij een dergelijk verzoek ontvangen. Dit is een positieve ontwikkeling. Het gaat hier echter maar om een klein percentage van alle medewerkers in DOWR-verband. Het verdient dan ook aanbeveling om dit soort verzoeken in 2023 op te nemen in de inwerkprogramma's en binnen NanoLearning een plek te geven. Ook is het aan te raden medewerkers ondersteuning te bieden doormiddel van werkinstructies, zodat zij daar op kunnen terugvallen bij het behandelen van een AVG-verzoek. Zo wordt geborgd dat ook nieuwe medewerkers en medewerkers die nog geen ervaring hebben met dit soort verzoeken kennis opdoen over de uitoefening van privacyrechten en de termijnen die moeten worden bewaakt.

Klachten

De AVG verplicht gemeenten om de naam en contactgegevens van de FG te publiceren zodat betrokkenen contact kunnen opnemen met deze functionaris. In 2022 hebben 13 personen van deze mogelijkheid gebruik gemaakt. De binnengekomen vragen en klachten over de AVG zijn door de FG onderzocht en afgehandeld. De meeste van de vragen en klachten gingen over:

- Het toepassen van de AVG door de betreffende gemeente (bijvoorbeeld: 'ik heb uit het nieuws begrepen dat gemeenten gegevens doorsluizen naar de VS. Mag dat zomaar?')
- De wijze waarop de betreffende gemeente bepaalde persoonsgegevens beveiligt (bijvoorbeeld: bij de gemeente Buren zijn gegevens gestolen via een leverancier. Kan dat bij mijn gemeente ook gebeuren?')
- Zorgen over het uitwisselen van gegevens (bijvoorbeeld: gegevens van mijn dochter zijn bij een andere partij terechtgekomen. Mocht de gemeente deze gegevens wel delen?')

De aard van de vragen en klachten ten opzichte van 2021 laat zien dat mensen zich steeds meer op basis van nieuwsberichten afvragen wat de gemeente met hun persoonsgegevens doet.

Security en privacy by design

In 2022 was te zien dat bij veel projecten de PO en ISO in de opstartfase werden betrokken. Bij sommige projecten resulteerde dat er niet in dat zij ook op tijd werden ingevlogen voor het daadwerkelijk op de naleving van de AVG en BIO toetsen van producten en diensten. Het op tijd aanhaken en aangehaakt houden van de ISO en PO bij de inkoop van een product of dienst en het doorlopen van aanbestedingsprocedures verdient dan ook blijvende aandacht in 2023.

Ontwikkelingen

Wet politiegegevens

Wanneer een gemeente haar taken uitvoert en daarbij persoonsgegevens verwerkt is bijna altijd de AVG van toepassing. Maar als een buitengewoon opsporingsambtenaar (BOA) persoonsgegevens verwerkt, dan ligt dat net even anders. Voor politiegegevens die onder de Wpg vallen geldt namelijk een ander strenger regime dan voor de persoonsgegevens die onder de AVG vallen.

Om te laten toetsen in hoeverre de drie gemeenten de verwerkingen die onder de Wpg vallen conform de wettelijke eisen hebben ingericht is er in 2022 een externe audit uitgevoerd over de periode 9 maart 2019 tot en met 31 december 2021. Uit deze nulmeting is gebleken dat de verwerkingen van politiegegevens binnen de drie gemeenten op veel vlakken nog niet aan de Wpg-eisen voldoen. De verwerkingen van politiegegevens zijn bijvoorbeeld nog niet opgenomen in de registers van verwerkingen, er is nog geen FG aangewezen voor het toezicht op de Wpg en er zijn nog geen wettelijk verplichte DPIA's uitgevoerd. De resultaten van de audit zijn naar de toezichthouder, de AP, gestuurd. Ondanks dat daarmee in kaart is gebracht welke stappen noodzakelijk zijn voor het implementeren van de Wpg in de drie gemeenten is er in 2022 nog geen begin gemaakt met de implementatie vanwege een gebrek aan capaciteit bij privacy.

Het advies is om in 2023 naast het opstellen van verbeterplannen, het uitvoeren van een hercontrole en een interne audit als drie organisaties aandacht te besteden aan een auditplan voor de komende jaren. Daarin wordt vastgelegd wanneer wordt gestart met de (voorbereidingen op) de verschillende audits, wie daarvoor het initiatief neemt/nemen, wie de audit uitvoeren, wie op de uitvoering toeziet, wat de doorlooptijd is en hoe de benodigde informatie (beveiligd) wordt opgeslagen. Hierin dient zowel de jaarlijkse interne audit als de vierjaarlijkse externe audit een plaats te krijgen.

Dreigingsbeeld 2023-2024

De drie belangrijkste dreigingen voor de lokale informatievoorziening die door de Informatiebeveiligingsdienst (IBD) in het tweejaarlijkse 'Dreigingsbeeld informatiebeveiliging gemeenten' worden gesignaleerd zijn:

- Meer ransomware-aanvallen met destructievere gevolgen;
    - Het fenomeen ransomware (gijzelsoftware) komt al jaren voor. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken.

- Steeds meer en ernstiger kwetsbaarheden in software;
    - Alle hard- en software bevat kwetsbaarheden en fouten. Deze zouden kunnen worden misbruikt door kwaadwillenden. Het is daarom zaak om kwetsbaarheden tijdig te verhelpen
- Weinig zicht op gevaren bij samenwerkingsverbanden en leveranciers.
    - Gemeenten vertrouwen erop dat bij een samenwerkingsverband informatieveiligheid en privacy ‘gewoon geregeld zijn’. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico’s als taken zijn uitbesteed. Gemeenten zijn in de afgelopen twee jaar regelmatig geconfronteerd met incidenten die ontstaan zijn bij derden waarbij de gevolgen in de eigen gemeente merkbaar waren.

In 2022 is het dreigingsbeeld 2023-2024 geplot op de drie organisaties. De resultaten zijn gebruikt om de informatiebeveiliging en de gegevensbescherming van de organisaties te verbeteren. Het advies is om in 2023 het continue analyseren van dreigingen voor de drie organisaties voort te zetten.

BIO 2.0 / NIS2

In 2022 heeft staatssecretaris Van Huffelen van Digitalisering middels een kamerbrief aan de Tweede Kamer laten weten dat de BIO de verplichte wettelijke basis voor informatieveiligheid bij de overheid moet worden. Deze BIO krijgt in 2023 een vernieuwing, namelijk de BIO 2.0. Concreet betekent dit dat een aantal hoofdstukken zal worden samengevoegd, een verandering in het aantal maatregelen en de aard van de maatregelen.

Ook op Europees vlak is er sprake van vernieuwing, namelijk de invoering van de NIS2 (Network and Information Systems 2). Met de invoering in 2025 zullen de regels voor de beveiliging van digitale diensten voor een breder toepassingsgebied gelden. Waar in de eerste versie dit met name gold voor essentiële bedrijven, zoals water- en telecombedrijven, geld dit nu ook voor (decentrale) overheden. De (decentrale) overheden zullen verplicht worden om meer maatregelen te nemen om cybersecurityrisico’s te beheersen. Daarnaast stelt de NIS2-richtlijn dat nationale autoriteiten de naleving van de regels uit NIS2 strenger moeten gaan handhaven. Indien men niet kan voldoen aan de richtlijn kunnen er boetes worden opgelegd, producten en/of diensten van de markt worden gehaald of management verantwoordelijk worden gehouden. Dit is vergelijkbaar met het toezicht dat de AP houdt op de naleving van de AVG.

Het verdient aanbeveling om in 2023 de ontwikkelingen op het vlak van de BIO 2.0 en NIS2 te blijven volgen, met name om medio 2025 aan de NIS2 te kunnen voldoen.

Crisisplan Cybersecurity

In 2022 zijn er stappen gezet met de vorming van het crisisplan van de gemeenten Deventer, Olst-Wijhe en Raalte. Het Strategisch Crisisplan Cybersecurity DOWR is bedoeld als leidraad voor bestuurders om op hoofdlijnen snel, efficiënt en adequaat inzicht en overzicht te creëren voor, tijdens en na een cybercrisis. In 2022 zijn onder andere de verschillende stakeholders bijeengekomen om de noodzaak van het plan te bespreken. Eind 2022 is de tekst en indeling van het plan vernieuwd. In 2023 zal er een afronding van het plan plaatsvinden in weer een gezamenlijke setting met de stakeholders. Een bevinding in 2022 was onder andere dat de verschillende nodige medewerkers uit de gemeenten onvoldoende waren aangesloten. Deze situatie zal in 2023 moeten worden verbeterd.

Het verdient aanbeveling om in 2023 uitvoerig met het crisisplan te oefenen, op zowel strategisch als tactisch niveau en zowel tekstueel (tabletop) als fysiek.

Rekenkameronderzoek

De Rekenkamercommissie van de gemeente Raalte heeft PBLQ gevraagd in 2022 onderzoek te doen naar de digitale weerbaarheid van de gemeente om mogelijke cyberaanvallen buiten de deur te kunnen houden en in het geval van een incident adequaat te kunnen reageren. Vanwege de samenwerking van de gemeente Raalte met de gemeenten Deventer en Olst-Wijhe op het gebied van bedrijfsvoering en ICT verdient het aanbeveling in 2023 de conclusies en aanbevelingen van PBLQ wat betreft de risico's op het gebied van informatieveiligheid en privacy met de twee andere gemeenten te delen. En zo nodig hier als gemeenten actie op te ondernemen.

Conclusie

De BIO en de AVG zijn omvangrijke en gecompliceerde normenkaders, die om structurele inzet vragen van bestuur, management en medewerkers. Uit dit toezichtjaarverslag komt naar voren dat de structurele inbedding van de informatieveiligheid- en privacygovernance en het risicomanagement bij de drie gemeenten nog volop in ontwikkeling is. De gemeenten hebben in 2022 stappen gemaakt in het beheersen van informatieveiligheid- en privacyrisico's ten einde de naleving van de BIO en de AVG in de werkprocessen te borgen. Evenals voorgaande jaren ging het daarbij vooral om het bestendigen van de reeds gehanteerde aanpak. Voor de Wpg stond 2022 vooral in het teken van een nulmeting in de vorm van een externe audit. Uit deze audit is gebleken dat de verwerkingen van politiegegevens binnen de drie gemeenten op veel vlakken nog niet aan de Wpg-eisen voldoen.

Er is in 2022 door de privacyorganisatie aandacht gevraagd voor voldoende capaciteit en middelen bij het uitvoeren van de verplichtingen onder de AVG en Wpg. Dit heeft uiteindelijk voor de budgetten gezorgd die in 2023 tot een capaciteitsuitbreiding bij privacy moeten gaan leiden. Dit betekent wel dat het gebrek aan capaciteit in 2022 op veel AVG-aandachtsgebieden invloed heeft gehad, zoals het actualiseren van het verwerkingsregister en het uitvoeren van DPIA's, en op het daadwerkelijk starten met de implementatie van de Wpg.

De CISO en de FG hebben in dit toezichtjaarverslag aanbevelingen gedaan bij de verschillende onderdelen van de BIO en de AVG. Deze zien er als volgt uit:

1. **Governance** Verbeter het eigenaarschap over privacy en informatieveiligheid bij het management
2. **Risicoanalyses** Voer DPIA's en Baselinetoetsen uit en registreer de resultaten
3. **Overzicht creëren** Actualiseer de drie registers van verwerkingen en pas dataclassificatie toe
4. **Bewustwording / Rechten van betrokkenen** Vergroot doormiddel van inwerkprogramma's en materie specifieke trainingen planmatig het bewustzijn

In het privacy- en informatiebeveiligingsplan 2023 wordt gekwalificeerd welke stappen de drie organisaties op het gebied van informatieveiligheid en privacy in 2023 willen gaan zetten.

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

Verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
Dit is de externe toezichthouder binnen Nederland met betrekking tot de uitvoering van de AVG.

Betrokkene
De persoon waarvan persoonsgegevens worden verwerkt.

Baseline Informatiebeveiliging Overheid (BIO)
De BIO beschrijft als normenkader het basisniveau voor informatiebeveiliging. De BIO wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Dit is één basisniveau voor informatiebeveiliging, één gezamenlijke taal voor alle overheidsorganisaties.

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. Een DPIA is verplicht voor 'risicovolle verwerkingen'. De AVG geeft aan voor welke categorieën van verwerkingen een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een aanvullend overzicht opgesteld waarin is geconcretiseerd in welke gevallen de organisatie verplicht is een DPIA uit te voeren.

Baselinetoets Basisbeveiligingsniveau (BBN)
Een instrument om informatieveiligheidsrisico's in kaart te brengen. Om te bepalen of een proces, informatiesysteem en/of informatie een bepaald Basis Beveiligings Niveau (BBN) heeft binnen de BIO, of meer maatregelen nodig heeft om risico's te minimaliseren.

Meldplicht datalekken
Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen moet het datalek binnen 72 uur na ontdekking worden gemeld bij de Autoriteit Persoonsgegevens. Dit wordt de meldplicht van datalekken genoemd.

Persoonsgegevens
Een persoonsgegeven is alle informatie, op wat voor manier ook, die iets zegt over een persoon. Bijvoorbeeld een naam, (mail)adres, woonplaats of geboortedatum, maar ook een loginnaam of een IP-adres.

Rechten van betrokkenen
Onder de AVG hebben mensen mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Het gaat om het recht op inzage, het recht op rectificatie en aanvulling, het recht op verwijdering, het recht op vergetelheid, het recht op beperking van de verwerking, het recht op een menselijke blik bij besluiten, het recht op dataportabiliteit, het recht om bezwaar te maken tegen de gegevensverwerking en het recht op duidelijke informatie over wat de gemeente met persoonsgegevens doet.

Verwerken van persoonsgegevens
Dit is in feite alles wat de gemeente doet met persoonsgegevens. Bijvoorbeeld het verzamelen, vastleggen, structureren, opslaan, wijzigen, opvragen of bekijken van persoonsgegevens.

Verwerkingsverantwoordelijke
Het gaat bij dit begrip om een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In deze rapportage gaat het bij de verwerkingsverantwoordelijke om het college van burgemeester en wethouders van de drie gemeenten.

Verwerkingsregister
Een gemeente is verplicht een register bij te houden van alle verwerkingen van persoonsgegevens. Dit register moet continu actueel worden gehouden. In het verwerkingsregister staan onder meer per structurele verwerking de verwerkingsdoeleinden, een beschrijving van de categorieën persoonsgegevens en de beoogde bewaartermijnen van persoonsgegevens.