Nota voor Burgemeester en Wethouders

Team: Concernstaf
Onderwerp:
Toezichtjaarverslag informatieveiligheid en privacy 2023

Notagegevens		
Bestuursorgaan	:	B-en-W 23-04-2024
Notanummer	:	2024-262
Datum	:	23-04-2024
Programma	:	11 - Bedrijfsvoering
Portefeuillehouder	:	Burgemeester,
Bijlage(n)	:	Privacy- en informatiebeveiligingsplan 2024.pdf,Toezichtjaarverslag CISO en FG 2023.pdf

Parafering

10-04-2024: Burgemeester
09-04-2024: Wethouder
09-04-2024: Chief information officer
18-04-2024: Burgemeester

Agendering

* 12-04-2024: Teammanager Concernstaf en Adjunct-secretaris
* 10-04-2024: Gemeentesecretaris/algemeen directeur
* 19-04-2024: Gemeentesecretaris/algemeen directeur
* 19-04-2024: Teammanager Concernstaf en Adjunct-secretaris

Definitieve akkoord

23-04-2024

B & W d.d.: 23-04-2024

Besluit

1. Het toezichtjaarverslag van de Chief Information Security Officer en de Functionaris Gegevensbescherming over 2023 vast te stellen en kennis te nemen van het privacy- en informatiebeveiligingsplan 2024
2. De raadsmededeling vast te stellen en met het toezichtjaarverslag en het privacy- en informatiebeveiligingsplan 2024 aan te bieden aan de gemeenteraad

De nota en het besluit openbaar te maken

Inleiding

Gemeenten zijn verantwoordelijk voor het gebruik van informatie en persoonsgegevens van inwoners, medewerkers en relaties. Het beschermen van deze gegevens is belangrijk en wordt gereguleerd door de Baseline Informatiebeveiliging Overheid (BIO), de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Niet-naleving kan ernstige gevolgen hebben, zoals schade aan het vertrouwen in de gemeente en haar bestuurders.

Om gegevens te beschermen en incidenten te voorkomen, houden de Chief Information Security Officer (CISO) en de Functionaris voor Gegevensbescherming (FG) toezicht. In het toezichtjaarverslag van 2023 constateren zij de positieve ontwikkelingen en voortdurende aandachtspunten op het gebied van informatiebeveiliging en privacy bij de gemeente Deventer, Olst-Wijhe en

Raalte.

De aanbevelingen voor 2024 richten zich op verschillende gebieden:

* Governance: Bewustwording vergroten, betrokkenheid van organisaties verhogen en periodieke sturingsinformatie delen met directie en bestuur.

* Privacy en security by design: Achterstanden wegwerken bij risicoanalyses, praktijk in lijn brengen met procedures en kennisniveau organisaties verhogen.

* Overzicht creëren: Registers bijwerken, capaciteit teams/domeinen aandacht geven en werkprocessen en informatiesystemen bijhouden.

* Incidenten: Lessen delen, schaduw-IT verminderen en integrale aanpak verzekeren bij applicatie- en dienstaanschaf.

* Bewustwording: Systematisch vergroten van bewustzijn en diverse bewustwordingsprikkels inzetten.

* Rechten van betrokkenen: Opnemen van omgang met politiegegevens in privacyverklaringen en aandacht vragen voor taken en verantwoordelijkheden bij verzoeken.

* Auditverplichting Wet politiegegevens: Starten met verbeterplannen en capaciteit teams/domeinen aandacht geven.

* Wet beveiliging netwerk- en informatiesystemen (Wbni): Capaciteit informatiebeveiliging voor implementatie van de NIS2-richtlijn aandacht geven.

Het toezichtverslag sluit af met specifieke aandachtspunten voor 2024 en een conclusie, waarin het belang van voortdurende inzet voor informatiebeveiliging en privacy benadrukt wordt. Met het vaststellen van het verslag komt er bestuurlijke steun voor de geplande acties op het gebied van privacy en informatiebeveiliging voor de gemeente Deventer. De bevindingen van de CISO en de FG, samen met de ervaringen van de informatiebeveiliging- en privacy adviseurs, liggen ten grondslag aan de acties in het jaarplan voor 2024. Het vaststellen van het jaarverslag is essentieel voor het succesvol uitvoeren van de plannen. Het jaarplan voor informatiebeveiliging en privacy wordt door de directie vastgesteld.

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, de AVG en de Wpg moeten daarbij in acht worden genomen.

Kader

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

Betrokken partijen en participatie

Toelichting op participatiebeleid

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

Financiële consequenties en dekking
Niet van toepassing.

Openbaarmaking en communicatie
Niet van toepassing.

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

RAADSMEDEDELING

Onderwerp	Toezichtjaarverslag informatieveiligheid en privacy 2023		
Nummer	2024-262	**Portefeuillehouder**	Burgemeester,
Team	DEV-CS	**Datum**	23-04-2024

Inleiding
Het college informeert uw raad over het toezichtjaarverslag informatieveiligheid en privacy over het jaar 2023. 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), de Wet Politiegegevens (Wpg) en de Baseline Informatiebeveiliging Overheid (BIO). De FG en CISO rapporteren hun bevindingen rechtstreeks aan het college van burgemeester en wethouders.

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

Kern van de boodschap
Om gegevens te beschermen en incidenten te voorkomen, houden de Chief Information Security Officer (CISO) en de Functionaris voor Gegevensbescherming (FG) toezicht. In het toezichtjaarverslag van 2023 constateren zij de positieve ontwikkelingen en voortdurende aandachtspunten op het gebied van informatiebeveiliging en privacy bij de gemeente Deventer. 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 binnen de gemeente. 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 (privacy risicoanalyses), het opzetten van een tool voor de registers van verwerkingen en het opstellen van een plan van aanpak voor de implementatie van de Wet Politiegegevens. Een groot deel van de gesignaleerde problemen vraagt echter ook in 2024 nog aandacht. De directie van gemeente Deventer onderschrijft de aanbevelingen van de CISO en FG en heeft deze naar acties vertaald voor 2024. Zij hebben het privacy- en informatiebeveiligingsplan 2024 omarmd.

Nadere toelichting
Gemeenten zijn verantwoordelijk voor het gebruik van informatie en persoonsgegevens van inwoners, medewerkers en relaties. Het beschermen van deze gegevens is belangrijk en wordt gereguleerd door de Baseline Informatiebeveiliging Overheid (BIO), de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Niet-naleving kan ernstige gevolgen hebben, zoals schade aan het vertrouwen in de gemeente en haar bestuurders.

De aanbevelingen voor 2024 richten zich op verschillende gebieden:

* Governance: Bewustwording vergroten, betrokkenheid van organisaties verhogen en periodieke sturingsinformatie delen met directie en bestuur.

* Privacy en security by design: Achterstanden wegwerken bij risicoanalyses, praktijk in lijn brengen met procedures en kennisniveau organisaties verhogen.

* Overzicht creëren: Registers bijwerken, capaciteit teams/domeinen aandacht geven en werkprocessen en informatiesystemen bijhouden.

* Incidenten: Lessen delen, schaduw-IT verminderen en integrale aanpak verzekeren bij applicatie- en dienstaanschaf.

* Bewustwording: Systematisch vergroten van bewustzijn en diverse bewustwordingsprikkels inzetten.

* Rechten van betrokkenen: Opnemen van omgang met politiegegevens in privacyverklaringen en aandacht vragen voor taken en verantwoordelijkheden bij verzoeken.

* Auditverplichting Wet politiegegevens: Starten met verbeterplannen en capaciteit teams/domeinen aandacht geven.

* Wet beveiliging netwerk- en informatiesystemen (Wbni): Capaciteit informatiebeveiliging voor implementatie van de NIS2-richtlijn aandacht geven.

Het toezichtverslag sluit af met specifieke aandachtspunten voor 2024 en een conclusie, waarin het belang van voortdurende inzet voor informatiebeveiliging en privacy benadrukt wordt. De directie van gemeente Deventer heeft de aanbevelingen van de CISO en FG overgenomen. Zij neemt haar verantwoordelijk door in 2024 het privacy- en informatiebeveiligingsplan 2024 uit te voeren.

Het toezichtverslag en het privacy- en informatiebeveiligingsplan worden als bijlage met deze raadsmededeling meegestuurd.

Privacy- en informatiebeveiligingsplan 2024

Voor u ligt het privacy- en informatiebeveiligingsplan voor 2024. In dit plan benoemen we de actiepunten op het gebied van privacy en informatieveiligheid voor de gemeenten Deventer, Olst-Wijhe en Raalte. Werkzaamheden in het kader van privacy en informatieveiligheid zijn slechts voor een deel vooraf te plannen. In een jaar gebeurt veel. Alledaagse gebeurtenissen en ontwikkelingen vragen vaak om inzet van de organisaties die niet vooraf was te voorzien. Denk aan beveiligingsincidenten, datalekken, inzageverzoeken en nieuwe applicaties of projecten die niet vooraf in beeld waren. Daarnaast gaat één van de Privacy Officers in 2024 een aantal maanden met verlof, waardoor de capaciteit bij privacy tijdelijk minder is. Bij het opstellen van dit document is hiermee rekening gehouden, om zo te komen tot een realistisch uit te voeren plan.
De bevindingen van de Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (CISO) uit het Toezichtjaarverslag en de ervaringen van de Privacy Officers (PO) liggen ten grondslag aan de actiepunten.

Wat willen we in 2024 bereiken?
Net zoals in 2023 is ook dit jaar de voornaamste doelstelling om beter inzicht te krijgen in de privacy- en informatiebeveiligingsrisico's. Dat betekent inzicht krijgen in de werkprocessen, hoe en met welke informatie er binnen deze processen wordt gewerkt en welke informatiesystemen daarbij worden gebruikt. Het gebruik van persoonsgegevens en andere soorten (gevoelige) informatie vindt immers plaats in bijna al onze werkprocessen. De gemeenten moeten zich hierover kunnen verantwoorden en daarmee voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Wet Politiegegevens (Wpg) en de Baseline Informatiebeveiliging Overheid (BIO).

Impact organisatie en kosten
Per actiepunt beschrijven we de impact op de organisatie (wie moet wat doen en wat zijn de succesfactoren?). De PO's en de Information Security Officer (ISO) nemen initiatief, maar zijn in veel gevallen afhankelijk van de inzet van andere medewerkers uit de teams of domeinen. Verder benoemen we de eventuele kosten van een actiepunt en of daarvoor dekking is.

Samenvattend overzicht

Aandachtsgebied	Actiepunt	Planning				pagina
1. Governance		**Q1**	**Q2**	**Q3**	**Q4**	3
	1.1 Actualiseren privacybeleid		X	X		3
	1.2 Vormgeven sturingsinformatie directies		X	X		3
2. Privacy en security by design		**Q1**	**Q2**	**Q3**	**Q4**	3
	2.1 Uitvoeren DPIA's op bestaande werkprocessen	X	X	X	X	3
	2.2 Verbeteren bewustwording m.b.t DPIA's op nieuwe werkprocessen			X		4
	2.3 Versterking digitale beveiliging met geoblocking	X				4
	2.4 Meer functionaliteit op laptops	X	X	X	X	4
	2.5 Zorgen voor een basisbeveiliging	X	X	X	X	5
3. Overzicht creëren		**Q1**	**Q2**	**Q3**	**Q4**	6
	3.1 Actualiseren verwerkingsregisters	X	X	X	X	6
	3.2 Implementeren dataclassificatie			X	X	7
4. Incidenten		**Q1**	**Q2**	**Q3**	**Q4**	7
	4.1 Crisisplan oefenen			X		7
	4.2 Pilot: sneller en beter reageren met Security AI	X				7
	4.3 Actualiseren procedure meldplicht datalekken		X			8
5. Bewustwording		**Q1**	**Q2**	**Q3**	**Q4**	8
	5.1 Uitvoeren verschillende bewustwordingsactiviteiten	X	X	X	X	8
6. Rechten van betrokkenen		**Q1**	**Q2**	**Q3**	**Q4**	9
	6.1 Opstellen werkinstructie AVG- en Wpg-verzoeken	X	X			9
7. Auditverplichting Wet Politiegegevens		**Q1**	**Q2**	**Q3**	**Q4**	9
	7.1 Uitvoeren zelfevaluatie Wet Politiegegevens				X	9
8. Wet beveiliging netwerk- en informatiesystemen		**Q1**	**Q2**	**Q3**	**Q4**	10
	8.1 Inzichtelijk maken impact NIS2 / ISO27001		X			10
	8.2 Implementeren risicomanagement / ISMS	X	X			10
	8.3 Organisaties toetsen met ENSIA		X			11
	8.4 Beleid uitlijnen in organisatie		X	X		11

De kosten voor de inzet van de Privacy Officer (PO), Information Security Officer (ISO), Functionaris Gegevensbescherming (FG) en Chief Information Security Officer (CISO) bij het uitvoeren van deze actiepunten zijn gedekt door de huidige bezetting. Bij een aantal actiepunten is ook personele inzet vanuit de betreffende teams of domeinen vereist. Dit staat per actiepunt beschreven. Mogelijke kosten die hierbij komen kijken vallen buiten de scope van dit plan. Dit kan per team of domein verschillen. Het is aan de betreffende manager om eventuele ontbrekende dekking te regelen.

1. Governance

1.1 Actualiseren privacybeleid

We actualiseren het privacybeleid van de 3 gemeenten uit 2018 en leggen dit opnieuw voor aan de drie colleges ter vaststelling. Waar nodig nemen we hierbij de eisen vanuit de Wet Politiegegevens mee. Verantwoordelijkheden op het gebied van privacy en informatieveiligheid brengen we hiermee opnieuw onder de aandacht bij het bestuur, de directie en het management.

Impact organisatie
De PO's stellen het beleid op en stemmen dit af met directie.

Kosten
Alleen personele kosten. Gedekt door huidige bezetting privacy.

Planning
Q2 – Q3 2024

1.2 Vormgeven sturingsinformatie voor directies

Naast het jaarlijkse toezichtverslag belandt informatie over de voortgang op het gebied van privacy en informatieveiligheid meestal toevallig op de bestuurs- en directietafels in de drie gemeenten. Om te voorkomen dat alleen de PO, ISO, FG en CISO zicht hebben op de stand van zaken, onderzoeken we met iedere gemeente samen hoe en welke sturingsinformatie periodiek met de directies kan worden gedeeld.

Impact organisatie
PO's en ISO onderzoeken met directies welke informatiebehoefte er is.

Kosten
Alleen personele kosten. Gedekt door huidige bezetting privacy en informatieveiligheid.

Planning
Q2 – Q3 2024

2. Privacy en security by design

2.1 DPIA's uitvoeren bestaande werkprocessen

In 2023 zijn alle managers[1] van de DOWR-gemeenten bijgepraat over de stand van zaken met betrekking tot het uitvoeren van DPIA's (privacy risicoanalyses) en is toegelicht hoe het uitvoeren van een DPIA in z'n werk gaat. Omdat niet op alle bestaande werkprocessen tegelijk DPIA's kunnen worden uitgevoerd, is door de PO's een prioritering voorgesteld. Hierin zijn o.a. de werkprocessen waar de Wpg op ziet meegenomen Deze prioritering wordt aangehouden en is als volgt[2]:

- 1: Jeugdwet, WMO, Participatiewet, Toezicht & Handhaving
- 2: Leerplicht/RMC, leerlingenvervoer, Beschermd Wonen
- 3: Vroegsignalering schulden, schuldhulpverlening, budgetbeheer.

Impact organisatie
De PO's nemen initiatief bij het uitvoeren van DPIA's op bestaande werkprocessen en begeleiden het proces. Een DPIA vereist echter ook inzet van het betreffende team of domein. Zowel bij het uitvoeren van de DPIA, als bij het implementeren van verbetermaatregelen in het werkproces. Gemiddeld gaat het om 13 uur per DPIA, afhankelijk van de complexiteit van het werkproces. De haalbaarheid van dit actiepunt is dan ook afhankelijk van de inzet en beschikbaarheid in de betreffende teams en domeinen.

[1] Met het begrip 'manager' wordt gedoeld op: teammanagers in Deventer, teamleiders in Olst-Wijhe, domeinmanagers in Raalte.
[2] De hieronder genoemde onderwerpen kunnen uit meerdere werkprocessen bestaan, waar dus ook meerdere DPIA's op uitgevoerd moeten worden.

Kosten
Personele kosten PO, ISO en FG zijn gedekt door huidige bezetting. Eventuele kosten binnen de teams of domeinen voor personele inzet of voor het implementeren van verbetermaatregelen vallen buiten de scope van dit plan. Dit kan per team en domein verschillen. Het is aan de betreffende manager om eventuele ontbrekende dekking te regelen.

Planning
Q1 – Q4 2024

2.2 Verbeteren bewustwording DPIA's nieuwe/gewijzigde werkprocessen

Het is de verantwoordelijkheid van proceseigenaren om nieuwe initiatieven die leiden tot een nieuw of gewijzigd werkproces met persoonsgegevens, aan te melden bij de PO's. De PO beoordeelt vervolgens of het uitvoeren van een DPIA verplicht is. Halverwege 2024 vragen we hiervoor opnieuw aandacht[3].

Impact organisatie
De PO's nemen initiatief om hierover te communiceren naar managers.

Kosten
Alleen personele kosten. Gedekt door huidige bezetting privacy.

Planning
Q3 2024

2.3 Versterking van digitale beveiliging met geoblocking

In lijn met ons beleid voor 2024 gaan we meer geoblocking toepassen, waarmee we specifieke landen toestaan om toegang te verkrijgen tot onze zakelijke omgeving. Deze maatregel is gericht op het verhogen van de beveiliging van onze digitale infrastructuur en het minimaliseren van potentiële bedreigingen vanuit bepaalde regio's. Door deze proactieve aanpak willen we de integriteit en vertrouwelijkheid van onze zakelijke gegevens versterken, en tegelijkertijd voldoen aan de noodzakelijke veiligheidsnormen en regelgeving. De landen worden op basis van informatiebeveiliging risicoanalyses toegevoegd (of verwijderd) van de blokkadelijst.

Impact organisatie
De ISO's zorgen voor de inrichting, vernieuwing en monitoring van geoblocking.

Kosten
Geen

Planning
Q1 2024

2.4 Meer functionaliteit op laptops

In 2024 streven we ernaar om op laptops meer apps toe te voegen, in overeenstemming met de geldende regels en normen. Ons doel is het omarmen van modern werken, terwijl we tegelijkertijd het zero trust-beveiligingsmodel handhaven. Hiermee willen we een flexibele werkomgeving creëren voor medewerkers, zonder de veiligheid van onze systemen en de vertrouwelijke informatie van inwoners en organisaties in gevaar te brengen.

Een essentiële maatregel die we implementeren op onze beheerde laptops is Multi-Factor Authenticatie (MFA). MFA versterkt de identiteitsverificatie door meerdere stappen, zoals het gebruik van een wachtwoord en biometrische gegevens, te vereisen voor toegang. Deze extra beveiligingslaag verhoogt aanzienlijk de bescherming tegen ongeautoriseerde toegang, waardoor het moeilijker wordt voor aanvallers om systemen en applicaties binnen te komen.

[3] Het uitvoeren van DPIA's op nieuwe of gewijzigde werkprocessen valt buiten de scope van dit plan.

Impact organisatie
De ISO's zorgen in samenwerking met o.a. M365 specialisten (DOWR-i) voor een implementatieplan met bijbehorende communicatie.

Kosten
In budget, onderzoek loopt of dit afdoende is.

Planning
Q1-Q4 2024

2.5 Zorgen voor een basisbeveiliging

We willen dat onze websites en mail goed beveiligd zijn. Daarom worden we regelmatig getoetst, ook door bijvoorbeeld basisbeveiliging.nl. Dit is een organisatie die controleert of onze publiek toegankelijk websites aan de gewenste normen voldoen. Op hun kaart kunnen we zien hoe we scoren op verschillende punten.

Begin 2023 waren we als DOWR-gemeenten groen gekleurd. In de loop van 2023 heeft de organisatie achter www.basisbeveiliging.nl een nieuw onderdeel toegevoegd aan de meting van gemeentelijke websites. Vanwege het gebruik van Google Analytics kleuren de gemeenten Deventer en Olst-Wijhe niet meer groen op de kaart van Nederlandse gemeenten. Gemeente Raalte scoorde nog wel groen vanwege het gebruik van een andere oplossing voor analytics. Hoewel het gebruik van Google Analytics niet betekent dat de privacy van de bezoeker niet gerespecteerd wordt, onderzoeken we in 2024 of we voor de websites van Deventer en Olst-Wijhe kunnen overstappen naar een andere oplossing voor analytics.

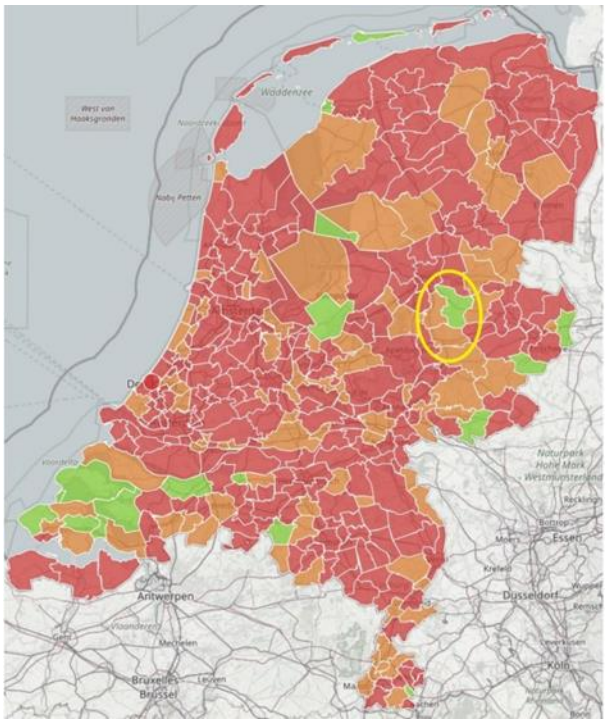
Sinds begin 2024 scoren alle gemeenten oranje. Dit komt door de mailbeveiliging. Dit willen we al enige tijd te verbeteren, maar we zijn afhankelijk van onze leverancier. Zij dienen hun inrichting aan te passen. Zij geven al enkele jaren aan dat ze dit van plan zijn, maar het is nog niet ingericht. We blijven erop aandringen, want we willen aan de normen voldoen. In 2024 blijven we hier actief op aansturen, ook bij partijen en contracten waar wij als organisaties een afhankelijkheid hebben.

Impact organisatie
De ISO's en CISO zorgen voor de opvolging en verbetering van de informatiebeveiliging van welke uit de verschillende audits, testen en adviezen naar voren komen. Indien het impact heeft op de organisatie zullen hier de nodige collega's aangesloten.

Kosten
Geen

Planning
Q1 - Q4 2024

In de kaart is het totaaloverzicht weergegeven van alle Nederlandse gemeenten in ***december 2023,*** met de DOWR-gemeenten geel omcirkeld.



1 - December 2023

3. Overzicht creëren

3.1 Actualiseren verwerkingsregisters

Het verwerkingsregister is een overzicht van alle structurele werkprocessen waarbij persoonsgegevens worden gebruikt. De huidige registers dateren uit 2018 en zijn sindsdien niet meer geactualiseerd. Naast dat het hebben van een actueel register een verplichting is vanuit de AVG, geeft het inzicht in hoe persoonsgegevens binnen de organisaties worden gebruikt en dient het als kapstok en verwijsindex voor de privacyboekhouding.
In januari 2024 is een tijdelijke inhuurkracht begonnen met de actualisatieslag van de 3 registers. Hierover zijn alle managers in de DOWR-gemeenten eind 2023 geïnformeerd. De actuele registers worden in een nieuw ontwikkelde tool in SharePoint opgezet. Hierin worden ook de Wpg-verwerkingen opgenomen. Daarnaast ontwikkelen we aan de hand van de opgedane ervaringen een werkwijze die borgt dat de registers actueel blijven. Managers worden zo veel mogelijk meegenomen in de actualisatieslag en bij het ontwikkelen van de eerdergenoemde werkwijze. Ook zal, waar het kan, de samenwerking worden gezocht met andere samenhangende informatievakgebieden, zoals informatiebeheer.

Impact organisatie
De tijdelijke inhuurkracht initieert en coördineert de actualisatieslag, met ondersteuning van de PO's. Daarnaast is input van medewerkers uit de teams en domeinen nodig. De inschatting is dat het gemiddeld 2 tot 4 uur kost per team of domein om de PO van voldoende informatie te voorzien. De haalbaarheid van dit actiepunt is afhankelijk van de inzet en beschikbaarheid in de teams en domeinen.

Kosten
De kosten voor tijdelijke inhuur zijn gedekt door incidenteel budget afkomstig uit het capaciteitsvoorstel privacy uit 2022.
Eventuele kosten voor personele inzet binnen de teams of domeinen vallen buiten de scope van dit plan. Dit kan per team en domein verschillen. Het is aan de betreffende manager om eventuele ontbrekende dekking te regelen.

Planning
Q1 – Q4 2024

3.2 Dataclassificatie toepassen

In 2024 implementeren we dataclassificatie. We categoriseren hiermee gegevens op vertrouwelijkheid, integriteit en beschikbaarheid. Zo kunnen we verschillende soorten informatie passend beveiligen.Het helpt ons als gemeenten om effectiever met informatiebeveiliging om te gaan en aan de regelgeving te voldoen. Ook zorgt dit ervoor dat we de privacy van burgers kunnen waarborgen. Het is wel noodzakelijk om gezamenlijk, met de verschillende experts, duidelijke beleidslijnen te ontwikkelen met betrekking tot dataclassificaties en deze beleidslijnen effectief te communiceren naar alle medewerkers.

Impact organisatie
Het succes van de implementatie vereist de betrokkenheid van verschillende belanghebbenden binnen de organisatie, waaronder IT-personeel, beleidsmakers, juridische experts en andere relevante afdelingen. De ISO's en CISO sluiten aan bij de verschillende initiatieven (zoals de 5 wetten) en nemen hier het belang van informatiebeveiliging mee.

Kosten
Ja, gedekt

Planning
Q3 - Q4 2024

4. Incidenten

4.1 Crisisplan oefenen

In 2024 oefenen we als DOWR ons Cybercrisisplan op zowel strategisch als tactisch niveau. Deze oefensessies, verspreid over verschillende bijeenkomsten met diverse belanghebbenden, zijn ontworpen om naadloos aan te sluiten op onze bestaande crisisplannen. Het doel is om de reactie op cybercrises te verbeteren en ervoor te zorgen dat onze teams op alle niveaus goed voorbereid zijn. Door specifiek te focussen op de dynamiek van een cybercrisis, willen we de veerkracht van onze gemeenten versterken tijdens een cybercrisis.

Impact organisatie
Belanghebbenden dienen deel te nemen aan verschillende oefensessies. De planning hiervoor zal ruim van tevoren worden afgestemd. De CISO zorgt voor de uitnodigingen, planning en sessies.

Kosten
Ja, gedekt

Planning
Q3 2024

4.2 Pilot: sneller en beter reageren met Security AI

We hebben begin 2024 gekozen om deel te nemen aan een pilot voor het inzetten van AI voor informatiebeveiliging. Door AI te integreren, kunnen we anticiperen en reageren op bedreigingen met een hogere snelheid, extra (AI) ondersteuning en nauwkeurigheid. Deze inzet biedt mogelijkheden om geautomatiseerde detectie en responsmechanismen te implementeren, wat niet alleen de bescherming van gevoelige informatie versterkt, maar ook onze wendbaarheid vergroot. Het is een stap naar het blijven waarborgen van een robuuste informatiebeveiliging.

Impact organisatie

De informatiebeveiligingspecialisten testen de inrichting en bruikbaarheid van AI-hulp tijdens het dagelijkse werk. De gedane ervaringen worden gedeeld in de organisatie.

Kosten
Ja, gedekt

Planning
Q1 2024

4.3 Actualiseren procedure meldplicht datalekken

De drie gemeenten hebben een procedure voor het melden van datalekken op grond van de AVG. Als een datalek plaatsvindt waarbij politiegegevens betrokken zijn is de Wpg daarop van toepassing. De procedure passen we hierop aan.

Impact organisatie
De PO's passen de procedure aan en communiceren dit naar de betreffende teams en domeinen die politiegegevens verwerken.

Kosten
Personele kosten PO zijn gedekt door huidige bezetting.

Planning
Q2 2024

5. Bewustwording

5.1 Uitvoeren verschillende bewustwordingsactiviteiten

Het blijven verbeteren van kennis en gedrag omtrent privacy en informatieveiligheid van alle medewerkers is van essentieel belang om onze organisaties veilig te houden. We werken op de volgende manieren aan bewustwording:

- *Nanolearning:*
  Het huidige Nanolearning programma loopt ook in 2024 door. De lessen worden steeds bijgewerkt en aangevuld op basis van de laatste ontwikkelingen. Zo nemen we ook lessen die we leren uit datalekken of andere informatiebeveiligingsincidenten op in het programma. We vragen opnieuw aan managers om Nanolearning onder de aandacht te brengen binnen hun team of domein. Hierin worden ze gefaciliteerd doormiddel van het aanleveren van rapportages (deelnamecijfers).
- *Weetje van Wessel*
  In de Intranet rubriek 'Weetje van Wessel' geeft de CISO op een laagdrempelige manier handige tips of informatie op het vlak van informatiebeveiliging, met als doel dat we steeds veiliger kunnen werken.
- *Red Teaming*
  Red teaming is een vorm van securitytesten waarbij een cyberaanval op een organisatie wordt nagebootst. Het doel is om de digitale weerbaarheid van de organisatie te meten en te verbeteren. Red teaming is een nuttige methode om de beveiliging van kritieke functies en systemen te testen en om het personeel te trainen in het herkennen en reageren op cyberaanvallen. In 2024 gaan we op een willekeurig moment dit inzetten.
- *Introductie:*
  Nieuwe medewerkers krijgen meer informatie over privacy en informatieveiligheid, waarbij ook het vorig jaar gemaakte animatiefilmpje makkelijker vindbaar wordt. Daarnaast onderzoeken we of er een periodieke introductietraining privacy en informatieveiligheid opgezet kan worden, vergelijkbaar met de trainingen 'Introductie Financiën' en 'De baas in huis' in Deventer. Deze kan worden gegeven door de Privacy Officer (PO) en de Information Security Officer (ISO).
- *Sharepointpagina privacy (kennisbank):*

Er is een Sharepointpagina opgezet. Deze Sharepointpagina wordt op dit moment gevuld met informatie en werkinstructies die zien op de toepassing van de AVG en Wpg. De pagina wordt voor alle medewerkers beschikbaar gemaakt.

- *Specifieke trainingen:*
  Bovenstaande bewustwordingsactiviteiten zijn generiek en voor alle medewerkers van toepassing. Maar de teams en domeinen hebben zo hun specifieke taken en dit vraagt dan ook om specifieke kennis en vaardigheden. Zo moeten bijvoorbeeld medewerkers in het sociaal domein continu zelf beoordelen welke persoonsgegevens in een bepaalde situatie verzameld moeten worden of uitgewisseld moeten worden met andere partijen. Dit vereist veel meer privacykennis dan bijvoorbeeld een medewerker die de meldingen openbare ruimte afhandelt. Op verzoek van de teams of domeinen geven we specifieke trainingen aan groepen medewerkers. Daarnaast kan de behoefte aan specifieke trainingen duidelijk worden uit de uitgevoerde DPIA's. Voor zover dat aan de orde is, worden deze specifieke trainingen opgezet en (periodiek) uitgevoerd door de PO en de ISO.

Impact organisatie
De PO’s en de ISO nemen initiatief in het opzetten van de bewustwordingsactiviteiten. Nanolearning vraagt om deelname van alle medewerkers. Ook het geven van specifieke trainingen vraagt om tijd en inzet van medewerkers binnen het team of domein. Wanneer dit aan de orde is, wordt dit met de betreffende manager afgestemd.

Kosten
Kosten voor Nanolearning programma zijn gedekt door het informatieveiligheidsbudget bij DOWR-i. Personele kosten PO en ISO zijn gedekt door huidige bezetting.

Planning
Q1 – Q4 2024

6. Rechten van betrokkenen

6.1 Opstellen werkinstructie AVG- en Wpg-verzoeken

We merken dat burgers steeds meer verzoeken op grond van de AVG indienen. Het gaat dan met name om inzageverzoeken waarbij een inwoner inzicht vraagt in de gegevens die de gemeente over deze persoon verwerken. Een inzageverzoek kan zeer omvangrijk zijn en daarmee veel vragen van de teams en domeinen. We merken dat het voor de teams en domeinen lang niet altijd duidelijk is wat hun rol is in het afhandelen van een AVG verzoek. Daarom werken we, in afstemming met de drie gemeenten, aan een duidelijke werkinstructie. Ook nemen we de verzoeken op grond van de Wpg hierin mee.

Impact organisatie
De PO’s nemen initiatief in het opstellen van de werkinstructie, maar zoeken hierbij afstemming met de gemeenten. Dit zodat de afhandeling van AVG- en Wpg-verzoeken op een manier gaat die het beste past bij iedere organisatie.

Kosten
Personele kosten PO zijn gedekt door huidige bezetting.

Planning
Q1 – Q2 2024

7. Auditverplichting Wet Politiegegevens

7.1 Uitvoeren zelfevaluatie Wet Politiegegevens

De Wpg heeft impact op de teams en domeinen waarbinnen boa’s werkzaam zijn en voor zover zij persoonsgegevens gebruiken ten behoeve van opsporingsdoeleinden. Voor dit jaar staat weer een verplichte zelfevaluatie op de planning voor Deventer en Olst-Wijhe, uitgevoerd door een externe

auditor. Raalte heeft sinds vorig jaar niet meer zelf een boa (leerplichtambtenaar) in dienst, maar huurt deze in waar nodig. We zoeken uit welke verplichtingen uit de Wpg nog van toepassing zijn voor de gemeente Raalte, nu zij niet langer meer zelf een boa in dienst hebben.

Impact organisatie
De PO's coördineren de zelfevaluatie en zijn contactpersoon voor de externe auditor. De betreffende teams wordt gevraagd input te leveren voor de zelfevaluatie in de vorm van een interview of het aanleveren van documenten.

Kosten
Personele kosten PO zijn gedekt door huidige bezetting. De inzet van de externe auditor brengt kosten met zich mee. Deze kosten worden gedekt vanuit de betreffende teams en programma's en vallen buiten de scope van dit plan.

Planning
Q4 2024

8. Wet beveiliging netwerk- en informatiesystemen (Wbni)

8.1 Inzichtelijk maken van impact NIS2 / ISO27001

Begin 2024 zijn de eerste stappen gezet voor ISO27001 certificering. Het werk dat wordt verricht voor de (mogelijk) ISO27001-certificering is als voorbereiding op de aanstaande NIS2 wetgeving (BIO 2.0/Wnbi). Het omvat op dit moment de afdelingen DOWR-i, FZ, en PSA. Door deze maatregelen kunnen we als DOWR gemeenten niet alleen aan regelgeving voldoen, maar ook informatiebeveiliging kwalitatief verbeteren en meer aantoonbaar maken.

Impact organisatie
De ISO's en CISO zijn actief aan het onderzoeken. Voorlopige bevindingen wijzen erop dat met name de informatiebeveiligings- en privacy specialisten worden belast. Dit is te wijten aan de noodzaak voor de organisatie om de werking van informatiebeveiliging meer aan te tonen.

Kosten
Ja, gedekt

Planning
Q2 2024 – Oplevering & Presentatie GAP analyse

8.2 Implementeren van risicomanagement/ISMS

Risicomanagement is het proces om de gevaren voor informatie te beheersen. Met risicomanagement maken we inzichtelijk welke gevaren er zijn, wat de impact hiervan kan zijn en hoe we de risico's kunnen weghalen of verminderen voor onze gemeentelijke processen. Een integraal onderdeel van risicomanagement is een ISMS (Information Security Management System). Met een ISMS kunnen we de risico's identificeren, analyseren, behandelen en monitoren. In 2024 gaan we de (al beschikbare) applicatie actief inzetten. Risicomanagement helpt ons als organisatie bij o.a. audits maar ook bijvoorbeeld de ENSIA.

Impact organisatie
De ISO neemt het voortouw met het in beeld brengen van de processen in de gemeenten. Samen met de privacyspecialisten worden de processen in beeld gebracht. Er is input van medewerkers uit de teams en domeinen nodig. De inschatting is dat het gemiddeld 2 tot 4 uur kost per team of domein om de ISO van voldoende informatie te voorzien. De haalbaarheid van dit actiepunt is afhankelijk van de inzet en beschikbaarheid in de teams en domeinen.

Kosten
Ja, gedekt

Planning
Q1 – Q2 2024

8.3 Organisaties toetsen met ENSIA

Burgers verwachten een betrouwbare overheid die zorgvuldig omgaat met informatie, met name op het gebied van het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). Deze waarborging draagt niet alleen bij aan betrouwbaarheid, maar ook aan de algehele kwaliteit en continuïteit van de bedrijfsvoering en dienstverleningsprocessen.

Wat staat er te gebeuren in 2024?

Er vinden veranderingen plaats in de audit van DigiD als onderdeel van ENSIA. Momenteel wordt de nadruk gelegd op de toetsing van opzet en bestaan. Deze aanpak verandert, en vanaf nu zal ook de werking worden getoetst. Dit betekent dat er niet langer alleen momentopnames worden beoordeeld, maar dat er over een uitgebreidere periode wordt gekeken naar de effectiviteit.

Impact organisatie
Er moet informatie opgehaald worden bij de ENSIA gerelateerde processen en diensten. Hier zijn al functionarissen aangewezen en actief bij aangesloten.

Kosten
Ja, gedekt

Planning
Q2 2024

8.4 Beleid uitlijnen in organisatie

Tijdens de ISO27001 nulmeting zijn al een aantal nodige acties naar boven gekomen. Hier werd duidelijk dat er beleid vanuit verschillende expertises in de organisatie zijn opgesteld, maar dat deze niet volledig op elkaar zijn uitgelijnd. Voor eind 2024, ter voorbereiding op de Wnbi, moeten de nodige beleidstukken zoveel mogelijk op elkaar zijn uitgelijnd. Denk hierbij aan bijvoorbeeld Toegangsbeveiliging Beleid vanuit informatiebeveiliging en toegangsbeveiligingsbeleid van Facilitaire Zaken. Deze stukken komen veel overeen, maar zijn op enkele punten nog verschillend.

Impact organisatie
De CISO, samen met de ISO's, zal op basis van de ISO27001 een actieplan opzetten om de verbeterpunten te implementeren. De mate van inzet die vereist is van de organisatie, varieert afhankelijk van het specifieke proces of beleid dat moet worden afgestemd op het huidige informatiebeveiligingsbeleid.

Kosten
Ja, gedekt

Planning
Q2 - Q3 2024

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.