

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.

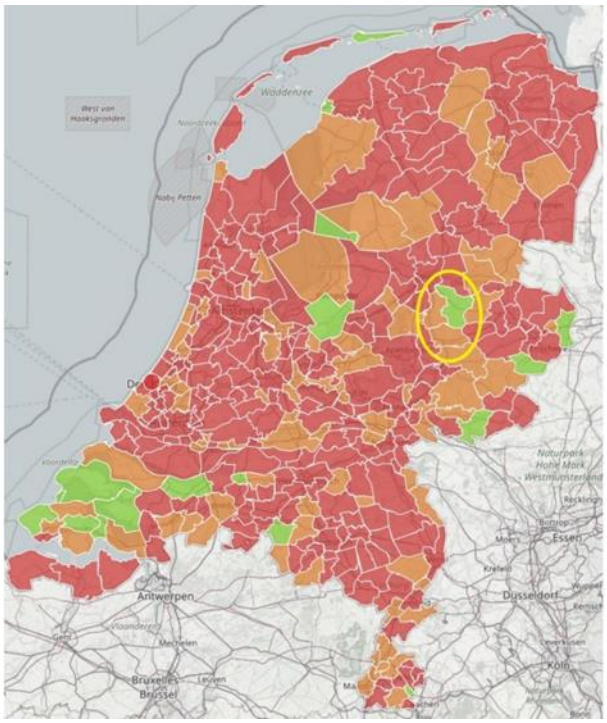
Sinds begin 2024 scoren alle gemeenten oranje. Dit komt door de mailbeveiliging. Dit willen we al enige tijd te verbeteren, maar we zijn afhankelijk van onze leverancier. Zij dienen hun inrichting aan te passen. Zij geven al enkele jaren aan dat ze dit van plan zijn, maar het is nog niet ingericht. We 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