Privacy- en informatiebeveiligingsplan

2023



DOWR - Lucas Klekamp - Privacy Officer (PO)

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



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

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

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

Wat willen we in 2023 bereiken?

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

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

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

Financiële consequenties

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

Impact organisatie

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

1. Gezamelijke actiepunten

1.1 Crisisplan

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

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

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

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

Kosten
Ja, gedekt

Planning
Q1 – Q4 2023

1.2 Bewustwording

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

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

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

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

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

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

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

Kosten
Ja, gedekt

Planning
Q1 – Q4 2023

1.3 Uitwerken werkwijze vastlegging verwerkingsregisters en risicoanalyses

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

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

Impact Organisatie
Nee

Kosten
Nee

Planning
Q2 2023

1.4 Uitvoeren risicoanalyses privacy en informatieveiligheid op bestaande werkprocessen

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

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

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

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

Kosten
Nee

Planning
Q3-Q4 2023

2. Actiepunten privacy

2.1 Actualiseren verwerkingsregisters

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

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

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

Kosten
Ja, gedekt

Planning
Q2 - Q4 2023

2.2 Actualiseren algemeen privacybeleid

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

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

Impact Organisatie
Nee

Kosten
Nee

Planning
Q3 2023

2.3 Uitwerken werkwijze doorbelasting uren DPIA

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

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

Impact Organisatie
Nee

Kosten
Nee

Planning
Q1 2023

2.4 Inrichten auditproces Wet Politiegegevens

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

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

Kosten
Ja, voorstel

Planning
Q2 2023

3. Informatiebeveiliging actiepunten

3.1 Beveiliging van mobiele apparaten

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

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

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

Impact Organisatie
Nee

Kosten
Ja, gedekt

Planning
Q2 2023

3.2 Monitoring en controle

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

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

Impact Organisatie
Nee

Kosten
Ja, gedekt

Planning
Q2 2023

3.4 Voorbereiding NIS2

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

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

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

Impact Organisatie
Nee

Kosten
Nee

Planning
Q4 2023

3.4 Actualisatie Informatiebeveiligingsbeleid

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

Impact Organisatie
Nee

Kosten
Nee

Planning
Q4 2023

3.5 Netwerk- en Firewallmigratie

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

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

Impact Organisatie
Nee

Kosten
Ja, gedekt

Planning
Q2 2023