Bijlage 1

Indicatoren
In dit deel van deze brief geven wij inzicht in de stand van zaken rond de thema's informatiebeveiliging en privacy binnen onze gemeente. Wij doen dit door dezelfde indicatoren die wij in onze brief van november 2024 besproken hebben opnieuw te behandelen.
Ten eerste zullen wij ingaan op lopende ontwikkelingen door deze te beschrijven aan de hand van de IT-roadmap (hierna: de roadmap). We geven een totaalbeeld van de naleving op het gebied van de BIO en de AVG. Tot slot bespreken we de KPI's die zijn afgestemd met de Raad en de Auditcommissie.

IT-roadmap
Om een overzicht te geven van de stand van zaken beschrijven wij de lopende ontwikkelingen aan de hand van de roadmap. Deze roadmap is samen met de accountant ontwikkeld als instrument om over risico's en maatregelen te rapporteren. Het gaat in de roadmap zowel over maatregelen op het gebied van informatiebeveiliging, als op het gebied van privacybescherming. In de roadmap zijn aanbevelingen en ambities omgezet in maatregelen die te volgen zijn door de tijd. Onderstaande acties zijn de acties in het kader van de roadmap. Dit is geen uitputtend overzicht van de lopende acties binnen onze gemeente.

In 2024 zijn de volgende acties afgerond:

- Het iVeiligheidsteam is aan de slag gegaan met autorisatiematrices, waarin is opgenomen welke medewerker welke bevoegdheid heeft. De controlerondes zijn bij een aantal afdelingen af.
- Het continuïteitsproject heeft voor alle afdelingen continuïteitsplannen opgeleverd. Bij een aantal afdelingen is ook in 2024 geoefend.
- Het iBewustzijn-communicatieplan is uitgevoerd. In 2024 omvatte dit onder andere een phishingcampagne, een iBewustzijnsonderzoek door Hogeschool Saxion en inzet op het gebied van het gebruik van Zivver.
- De herhalings eLearning voor Informatiebeveiliging en Privacy is op Studytube beschikbaar gesteld. 60% van de medewerkers heeft deze gevolgd.
- In 2024 is twee keer een informerende brief naar de raad gestuurd met betrekking tot de gekozen KPI's.
- Het NYMACON hack evenement heeft bij Waalhalla in Nijmegen plaatsgevonden. De evaluatie met de studenten en iRvN was positief.
- iRvN is aan de slag met het traject naar certificering op basis van de BIO. Een achttal processen is getoetst. De demarcatielijst waarmee verantwoordelijkheden over iRvN en de gemeenten worden afgebakend is compleet.
- De CISO heeft in 2024 haar controleplan uitgevoerd en hier over gerapporteerd aan het GMT en de directie. Dit controleplan had betrekking op de processen van autoriseren, het afhandelen van incidenten en wijzigingen.
- Het team Stadscontrol ziet toe op het opvolgen van bevindingen en het nemen van de juiste maatregelen. Dit gebeurt door het voeren van adviesgesprekken, het begeleiden van prestatiedialogen en het toetsen van maatregelen, bijvoorbeeld door het uitvoeren van interne audits met behulp van de CyberManager en het uitvragen door de FG en de CISO.
- We betrekken de Privacy officer inmiddels actief bij intakes, zodat vooraf gesignaleerd kan worden of een DPIA noodzakelijk is en privacy by design geïmplementeerd kan worden.

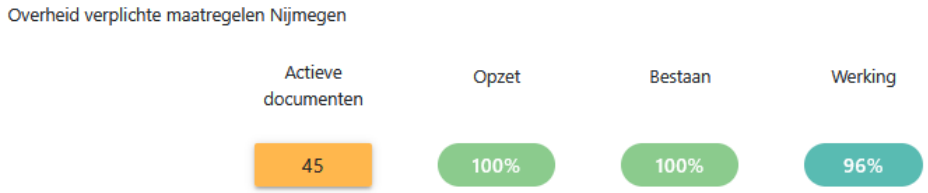
De volgende acties lopen op dit moment:

- Bij een aantal afdelingen wordt de controle van de autorisaties nog ingericht. Verbeteringen in het proces naar aanleiding van de vorige ronde worden toegepast op de rondes van 2025.

- De laatste continuïteitsplannen worden begin 2025 geoefend. De eerder opgestelde plannen worden geüpdatet met de aanbevelingen uit de oefeningen. Deze worden aangeleverd om te verwerken tot een gemeentebreed continuïteitsplan.
- Het bestaande informatiebeveiligingsbeleid wordt geactualiseerd. Geplande vaststelling is in 2025.
- Ook in 2025 zal de gemeentebrede eLearning worden uitgezet en zullen iBewustzijnsacties worden uitgevoerd (zoals een lezing door Daniel Verlaan). Daarnaast zal er extra aandacht zijn voor het bewustzijn van het management en het bestuur, door crisisoefeningen te doen met de MT's van alle afdelingen.
- Het overzicht van projecten en maatregelen zal herzien worden aan de hand van de huidige ontwikkelingen om de IT Roadmap opnieuw te vullen.
- BIO2 (de opvolger van het huidige normenkader voor informatiebeveiliging) zal worden geïmplementeerd via ons Information Security Management Systeem (ISMS) CyberManager.
- We werken aan een compleet overzicht van de verschillende privacy-overeenkomsten die we hebben, zoals verwerkersovereenkomsten en privacy protocollen.

Totaalscores vanuit CyberManager

De CyberManager is een applicatie die wij gebruiken als Information Security Management System (ISMS) en als Privacy Information Management System (PIMS). In deze applicatie houden we de voortgang op de naleving van de BIO en de AVG bij. De applicatie geeft voor beide onderwerpen een totaalscore als het gaat om opzet, bestaan en werking van de geïmplementeerde maatregelen op beide vlakken.



Figuur 1 status informatiebeveiliging 2025



Figuur 2 status privacy

Informatiebeveiliging

De scores zoals hierboven weergegeven voor Informatiebeveiliging (opzet, bestaan en werking) zijn gegeven op basis van BIO versie 1.04. Voor opzet en bestaan is het 100%, maar voor werking is dit niet zo. Bij de toetsing op basis van BIO 1.04 zijn alleen de verplichte overheidsmaatregelen meegenomen. Het feit dat opzet en bestaan van deze maatregelen 100% zijn, betekent dat we bij de maatregel beschreven hebben hoe we deze uitvoeren (opzet) en een voorbeeld kunnen laten zien dat dit ook zo is gebeurd (bestaan). De werking is nog geen 100%, want dat zou betekenen dat het proces altijd goed wordt uitgevoerd. In deze toetsing werken we risicogestuurd, wat wil zeggen dat we de opzet het meest kritisch beoordelen bij de meest risicovolle processen. Dit heeft te maken met beperkingen in de capaciteit door onze gehele organisatie (eerste, tweede en derde lijn), maar ook bij iRvN, die een deel van de (technische) maatregelen voor de gemeenten in de regio beheert.

De conclusie is dat wij in 2024 goed scoren op onze KPI's, maar vanwege de ontwikkelingen beschreven in het eerste deel van deze brief is het onze verwachting dat deze score zal dalen. In de tweede raadsinformatiebrief voor

2025 zullen we meer duidelijkheid kunnen geven over de effecten van de ontwikkelingen zoals de Cyberbeveiligingswet op de KPI's.

Privacy

Bij privacy is de score ten opzichte van de vorige brief wat veranderd. Deze keer is de interne audit, zoals in de vorige brief aangekondigd, voor het eerst gedaan aan de hand van het IBD Borgingsproduct 3.0. In de vorige brieven was dat nog aan de hand van het borgingsproduct 2.0. Zoals eerder in deze brief aangegeven zijn er in het borgingsproduct 3.0 vereisten die in het oude product niet gevraagd werden. Voor sommige van die vereisten is er dan ook nog geen opzet, en dus ook geen bestaan. Daarom zijn de scores voor opzet en bestaan geen 100% meer. De werking is gelijk gebleven op 54%. De trend vanuit de vorige brieven blijft daarmee overeind. Qua opzet en bestaan scoren we redelijk goed, maar de werking aantonen blijkt in de praktijk een heel stuk lastiger.
De volgende interne audit vindt weer plaats aan het einde van 2025. Daarom is de verwachting dat in de volgende brief de scores weinig zullen veranderen ten opzichte van nu.

KPI's om mee te sturen

Er zijn op hoofdlijnen drie aandachtsgebieden vastgesteld:

1. Gegevensbeheer
2. Personeel
3. Toegangsbeveiliging (zowel fysiek als digitaal)

De hierboven genoemde aandachtsgebieden zijn door de raadsleden uitgekozen als thema's die de komende periode extra aandacht verdienen.

1. KPI's vanuit privacy

Gegevensbeheer is het eerste thema. Het heeft zowel componenten van informatiebeveiliging als van privacy in zich. We delen gegevensbeheer op in twee onderdelen die beide van grote invloed zijn hierop. Dat zijn DPIA's en het voldoen aan de privacy-eisen op het gebied van wetgeving en contracten.
In het borgingsproduct 3.0 is het thema DPIA's opgedeeld in vier sub-KPI's, namelijk 'Procedure DPIA', 'DPIA register', 'Overzicht maatregelen DPIA's' en 'DPIA Documenten'. Deze worden onder onderdeel a toegelicht. De privacy-eisen op het gebied van wetgeving en contracten zijn opgedeeld in drie sub-KPI's, namelijk 'Overzicht convenanten bij samenwerkingsverbanden', 'Actueel overzicht verwerkersovereenkomsten' en 'Overzicht periodieke controle en bevindingen'. Die worden nader toegelicht onder b. Voor al deze sub-KPI's geldt dat opzet en bestaan in de cybermanager 100% scoren. Daarom wordt hieronder enkel de score van de werking zoals bekend in de CyberManager weergegeven.

a. DPIA's

Een Data Protection Impact Assessment (DPIA) is een privacy scan die een gegevensverwerking van start tot eind in beeld brengt. Er zijn tot nu toe 103 DPIA's uitgevoerd.

i. Procedure DPIA

Er is een procedure vastgesteld die doorlopen moet worden zodra er gestart wordt met een DPIA. Deze procedure wordt doorgaans goed gevolgd. De score is dan ook 100%.

ii. DPIA register

Er is een register waar alle DPIA's en bijpassende oordelen die we hebben vindbaar zijn. Het register dat voor alle collega's te raadplegen is, is echter nog niet up-to-date en moet nog aangevuld worden. De score is 75%.

iii. Overzicht maatregelen DPIA's

Uit DPIA's volgen doorgaans maatregelen die de privacy risico's binnen gegevensverwerkingen moeten mitigeren. Deze maatregelen worden opgenomen in het oordeel van de FG. Die staan centraal opgeslagen in het DPIA register. De score is 75%.

iv. DPIA documenten

Er zitten vaak verschillende bijlagen bij DPIA, zoals overeenkomsten of procesbeschrijvingen. Deze documenten worden centraal opgeslagen in het register wat de FG bijhoudt. Op het openbare register staan niet alle bijbehorende documenten erbij, slechts de DPIA en het oordeel. De score is 75%.

b. Privacy-eisen wetgeving en contracten

Deze KPI gaat over verwerkersovereenkomsten en andere soorten privacy-overeenkomsten (denk aan privacy protocollen en overeenkomsten onder gezamenlijke verantwoordelijkheid). Dit jaar worden alle privacy-overeenkomsten getoetst op naleving door de FG.

i. Overzicht convenanten bij samenwerkingsverbanden

Bij samenwerkingsverbanden maken we doorgaans aanvullende afspraken in de vorm van privacy protocollen of convenanten. Wanneer team privacy betrokken wordt, gebeurt dit. We hebben een overzicht van deze convenanten, maar kunnen niet garanderen dat deze compleet is. De score is 75%.

ii. Actueel overzicht verwerkersovereenkomsten

We hebben steeds beter overzicht van welke verwerkersovereenkomsten we allemaal hebben. We hopen dit jaar voor het eerst een compleet en actueel beeld te hebben, maar dat is er nog niet. De score hier is 75%.

iii. Overzicht periodieke controle en bevindingen

Dit jaar worden voor het eerste alle verwerkersovereenkomsten getoetst op naleving. In vorige jaren was dit slechts een steekproef. In de praktijk blijft het nog zeer lastig aantoonbaar dat de gemaakt afspraken ook daadwerkelijk nageleefd worden. De score is 50%.

2. KPI's vanuit informatiebeveiliging

a. *Gegevensbeheer*

Voor gegevensbeheer vanuit het perspectief van informatiebeveiliging kijken we vooral naar het veilig verwijderen van gegevens en het risicobewust classificeren van gegevens.
Het veilig verwijderen van gegevens heeft betrekking op wat er gebeurt met gegevensdragers op het moment dat deze niet meer gebruikt worden. Het gaat daarbij om bijvoorbeeld gegevensdragers in computers (bijvoorbeeld de "harde schijf"), maar het kan ook gaan om USB-sticks (die bijvoorbeeld gevonden worden) of andere dragers. In de CyberManager scoort het veilig verwijderen van gegevens op dit moment 100%.
Gegevensbeheer is niet mogelijk zonder classificatie van informatie. Bij het classificeren van informatie wordt bepaald welk niveau van vertrouwelijkheid, integriteit en beschikbaarheid bij deze informatie hoort. Het is de enige manier om te kunnen bepalen welke informatie wanneer vernietigd moet worden. In de CyberManager scoort de classificatie van informatie op dit moment 100%.

b. Personeel

Personeel is het tweede thema. Hierbij wordt met name gevraagd om aandacht voor het iBewustzijn van de medewerkers, de basis onder veel maatregelen die afhankelijk zijn van de medewerking van het personeel. Dit heeft ook raakvlakken met privacy. Medewerkers moeten weten hoe gevoelig de informatie is waar zij mee werken, zij moeten tijdig de nodige trainingen volgen op het vlak van informatiebeveiliging en privacy. In de CyberManager scoort bewustzijn, opleiding en training ten aanzien van informatiebeveiliging qua opzet en bestaan 100%, maar op werking 50% vanwege de dalende deelname aan de herhalingstraining.
Het juist behandelen van bedrijfsmiddelen en informatie scoort wel 100% in de CyberManager.

c. Toegangsbeveiliging

Het derde thema is toegangsbeveiliging. Dit kent twee aspecten: de fysieke toegangsbeveiliging (3a) tot de gebouwen en beveiligde zones binnen de gebouwen. In de CyberManager scoort deze qua opzet en bestaan 100% en voor werking 75%. De zonering in Marienbeurs wordt binnenkort verbeterd.
De digitale toegangsbeveiliging (3b) heeft betrekking op toegang tot applicaties en data. Deze is gebaseerd op de juiste omgang met accounts, wachtwoorden en multi-factor authenticatie. De huidige status van de digitale beveiliging in de CyberManager is 100%.