

Aan de gemeenteraad van Nijmegen

Postadres

Gemeente Nijmegen
Postbus 9105
6500 HG Nijmegen

Bezoekadres

Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactpersoon

Esther Zijlstra
e.zijlstra@nijmegen.nl
T 024 – 329 39 63

Ons kenmerk

E25.002254

Datum 28 oktober 2025
Onderwerp Voortgang op informatiebeveiliging en
privacy

Geachte leden van de raad,

Zoals met uw raad afgesproken stuurt het college u twee keer per jaar een brief met daarin de stand van zaken op het gebied van Informatiebeveiliging en privacy. In de brief van april 2025 concludeerden we dat er meer van ons gevraagd wordt dan we kort na het rekenkameronderzoek, dat aanleiding was voor deze brieven, hadden verwacht. We kondigden aan dat we in het begrotingsproces in beeld gingen brengen wat naar onze indruk nodig was om de gestelde doelen alsnog te bereiken. Dat hebben we inmiddels gedaan. De begroting is op het moment van schrijven nog niet vastgesteld en we zijn nog in afwachting of de gevraagde middelen beschikbaar zullen komen. De enigszins dalende scores van de KPI's zijn een gevolg van de trends die wij in april signaleerden.

In deze uitgave van de raadsinformatiebrief over de voortgang op informatiebeveiliging en privacy geven we inzage in de lopende ontwikkelingen, door deze te beschrijven aan de hand van de IT-roadmap (hierna: de roadmap). Daarnaast schetsen we een totaalbeeld van de compliance op gebied van de AVG en de Baseline informatiebeveiliging overheid (BIO). Dit doen we op basis van de huidige versies van de normenkaders, wetend dat volgend jaar met de Cbw versie 2 van de BIO wettelijk verplicht wordt. Tot slot geven we inzicht in de KPI's die met uw raad zijn afgestemd en later zijn bevestigd door de Auditcommissie. Over het algemeen kunnen we voor informatiebeveiliging stellen dat, waar scores gedaald zijn, dit komt omdat we met de nieuwe norm in gedachten geoordeeld hebben. Daarnaast is het zo dat iRvN zich dit jaar voor een aantal processen. laat certificeren. Hun nieuwe manier van verantwoorden is nog niet verwerkt in ons systeem, de CyberManager.

IT-roadmap

De 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 over maatregelen op het gebied van privacybescherming. In de roadmap zijn aanbevelingen en ambities omgezet in maatregelen die te volgen zijn door de tijd. Onderstaande acties volgen uit de roadmap. Dit is geen uitputtend overzicht van de lopende acties binnen onze gemeente, maar een

selectie van acties waarop de voortgang is geboekt. In de jaarrapportage op het gebied van informatiebeveiliging zal op sommige acties verder worden ingegaan.

In 2025 zijn tot en met september de volgende acties afgerond:

- Tweemaal jaarlijks de Raad informeren over de stand van zaken op privacybescherming en informatiebeveiliging;
- In de conceptbegroting is in beeld gebracht welke extra middelen nodig zijn om onze ambitie te behalen;
- Met prioriteit afronden van een groot deel van de 'must have' DPIA's¹;
- Aanbieden van een nieuwe gemeentebrede leerlijn over de afhandeling van datalekken (deelname score 76%);
- Project iBewustzijn met hogeschool Saxion afgerond. Workshop opgeleverd;
- Kritische prestatie indicatoren doorgezet;
- We hebben een medewerker geworven die de kwaliteit van interne audits en registraties gaat bevorderen;
- Gemeenschappelijke uitvraag Controlplan FG en CISO gedaan.

De volgende acties lopen op dit moment:

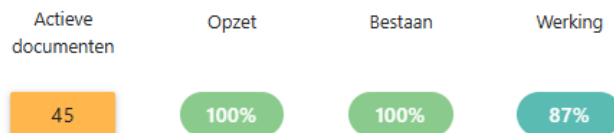
- Continuïteitsplan gemeentebreed herzien en oefenen;
- Het bezoeken van de MT's om te oefenen met casuïstiek op het gebied van iVeiligheid (afronding gepland Q1 2026);
- Het bestaande informatiebeveiligingsbeleid wordt geactualiseerd. Geplande vaststelling volgt eind 2025;
- Verwerkersovereenkomsten en privacy analyses zullen verder worden uitgewerkt en ook getoetst;
- Van privacygevoelige applicaties worden autorisatie matrices opgesteld, met inachtneming van functiescheiding. Verbeteringen in het proces worden toegepast voor de rondes van 2025;
- Verbeterslag op ISMS wordt uitgevoerd en plan voor implementatie Cbw is gemaakt.

Totaalscores vanuit CyberManager

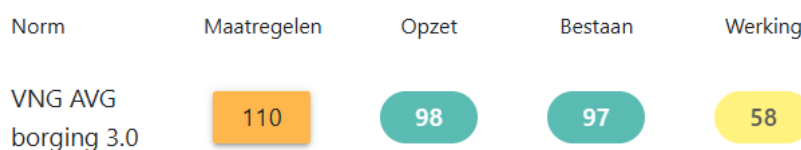
De CyberManager is een applicatie die wij gebruiken als Information Security Management System (ISMS) en als Privacy Information Management System (PIMS). In deze applicatie houden we de voortgang op de naleving van de BIO en de AVG bij. De applicatie geeft voor beide onderwerpen een totaalscore als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

¹ De Informatiebeveiligingsdienst (IBD) heeft een lijst gepubliceerd met onderwerpen waarvoor elke gemeente een DPIA zou moeten hebben.

Overheid verplichte maatregelen Nijmegen



Figuur 1 status informatiebeveiliging



Figuur 2 status privacy

Informatiebeveiliging

Zoals hierboven te zien zijn de scores voor opzet en bestaan 100%, maar is dit voor werking niet zo. Het is belangrijk om hier een aantal kanttekeningen bij te maken.

De toetsing voor deze score is gedaan aan de hand van het geldende BIO normenkader 1.04. Daarbij zijn alleen de verplichte overheidsmaatregelen meegenomen, weergegeven in de “actieve documenten” hierboven. 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 geen 100%, want dat zou betekenen dat het proces altijd goed wordt uitgevoerd. En dat is niet zo. In de toetsing werken we risico gestuurd, 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. Dit betekent dat er met name als het gaat om werking voor de gemeente nog verbetering mogelijk is bij processen die niet tot de meest kritische, maar wel gevoelige, processen behoren. Ook deze processen maken ons kwetsbaar.

De verwachting is dat de implementatie van de nieuwe Cyberbeveiligingswet (Cbw) in Q2 van 2026 zal betekenen dat de scores zullen verslechteren. Omdat gemeenten onder deze wet als ‘essentiële entiteiten’ worden aangemerkt zal de lat steeds hoger komen te liggen. Bepaalde taken die gemeenten vervullen moeten onder alle omstandigheden door blijven gaan. De hogere eisen gelden met name voor continuïteit en de omgang met leveranciers. Daarnaast neemt het risico vooral voor het fysieke domein toe. Apparatuur in dit domein is steeds vaker doelwit van aanvallen. Bovendien neemt met de wetgeving ook het toezicht toe en daarmee de kans op een boete. Het aantal en de zwaarte van de te treffen maatregelen om dit risico te bestrijden wordt daarom vergroot. Vanaf de tweede raadsbrief in 2026 maken we dat voor u inzichtelijk.

Privacy

De scores ten opzichte van de brief van 1 april zijn licht verbeterd op het gebied van opzet en bestaan. In december komt de jaarlijkse interne audit weer aan bod, waardoor we in de volgende raadsbrief van het voorjaar grotere verschillen verwachten. Wat we wel blijven zien, is dat het lastig blijft om de werking aan te tonen. Dit betekent dat we veelal een plan hebben om AVG-proof te worden en dat deze plannen ook deels functioneren. Het lukt alleen nog niet consequent om dat achteraf ook aan te kunnen tonen. Dat betekent dat in het vastleggen van afspraken en het naleven van afspraken nog veel winst te behalen valt.

KPI's om mee te sturen

Nu wij een totaalbeeld hebben geschetst van de informatiebeveiliging en de privacybescherming binnen onze gemeente, gaan we in op de KPI's die in overleg met de Raad zijn uitgekozen om op te sturen. Deze KPI's zijn uitgekozen op basis van aandachtsgebieden die in het bovengenoemde rekenkameronderzoek 'Weten wat je moet weten' naar voren kwamen, gecombineerd met prioriteiten die aangegeven werden door raadsleden binnen de domeinen van informatiebeveiliging en privacybescherming. Het maken van keuzes binnen deze domeinen is essentieel om wezenlijke vooruitgang te kunnen boeken en om effectief te kunnen sturen.

Er zijn op hoofdlijnen drie aandachtsgebieden vastgesteld:

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

Zoals hieronder te zien kan men op deze gebieden inzoomen op meetbare KPI's. In de toelichting wordt stilgestaan bij de ontwikkeling van de KPI's en de subonderdelen.

1. KPI's vanuit privacy

Gegevensbeheer is het eerste thema. Dit 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.

a. DPIA's

Een Data Protection Impact Assessment (DPIA) is een privacy scan die een gegevensverwerking binnen een proces of project van start tot eind in beeld brengt. Er zijn tot nu toe 116 DPIA's uitgevoerd. Dat zijn er sinds de laatste raadsbrief 13 extra. We prioriteren bij de DPIA's de must have DPIA's.

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%. Dit was in de vorige brief ook al zo.

ii. DPIA register

Er is een register waar alle DPIA's en bijpassende oordelen die we hebben vindbaar zijn. Het register dat voor alle medewerkers te raadplegen is inmiddels up to date, dat was in april nog niet zo. Dit werkt echter nog niet door in de score omdat de interne audit nog niet geweest is. De score is daarom in de Cybermanager nog steeds 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 ongewijzigd en blijft 75%.

iv. DPIA documenten

De score hier is ongewijzigd ten opzichte van de laatste brief en blijft dus 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 zijn alle privacy-overeenkomsten getoetst op naleving door de FG. Dit is onlangs met uw raad gedeeld middels het controlplan van de FG over 2024.

i. Overzicht convenanten bij samenwerkingsverbanden

Bij samenwerkingsverbanden maken we doorgaans aanvullende afspraken in de vorm van privacy protocollen of convenanten. Middels de uitvraag voor het controlplan hebben we een overzicht gecreëerd van convenanten bij samenwerkingsverbanden. Deze is grotendeels compleet, maar vanuit verschillende organisatieonderdelen nog niet. De score is 75%.

ii. Actueel overzicht verwerkersovereenkomsten

We hebben steeds beter overzicht van welke verwerkersovereenkomsten we allemaal hebben. De score hier is ongewijzigd en blijft 75%.

iii. Overzicht periodieke controle en bevindingen

Dit jaar zijn alle bij ons bekende verwerkersovereenkomsten getoetst op naleving. In vorige jaren was dit slechts een steekproef. Uit deze toetsing is duidelijk geworden dat de naleving van verwerkersovereenkomst nog laag is. De score is 50%.

2. KPI's vanuit informatiebeveiliging

Voor **gegevensbeheer** vanuit het perspectief van informatiebeveiliging kijken we vooral naar het veilig verwijderen van gegevens en het risicobewust classificeren van gegevens.

1a Veilig verwijderen 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 gevonden worden) of andere dragers. iRvN heeft een overeenkomst met D-two voor het gecertificeerd wissen en zo mogelijk opnieuw inzetten van apparatuur die door ons niet meer gebruikt wordt. Deze werkwijze is in het afgelopen jaar niet veranderd. De score is 100%.

1b Classificatie van informatie

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. Applicaties en de data die daarin gebruikt wordt zijn geclassificeerd volgens de standaard die door de Informatiebeveiligingsdienst voor gemeenten (hierna de IBD) gebruikt wordt. Dit proces is gedocumenteerd en de resultaten zijn goedgekeurd door de eigenaren van de applicaties. De werkwijze is niet veranderd. Wel groeit het aantal betrokken systemen. Bovendien zal het opruimen van de ongeclassificeerde informatie in het kader van Microsoft 365 nog enige tijd duren. De score op werking is 50% omdat nog niet van alle kritieke systemen jaarlijks de classificatie opnieuw beoordeeld wordt.

Personeel is het tweede thema. Hierbij wordt met name gevraagd om aandacht voor het iBewustzijn (a) 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 en daarnaar handelen (b). Ook hier geldt dat een score van 100% niet betekent dat alle medewerkers een perfect iBewustzijn hebben.

2a iBewustzijn

Er is een scholingsprogramma (eLearning), dat medewerkers volgen waarbij zij relevante informatie krijgen over wat gevoelige informatie is en hoe daar mee te werken. Er zijn ook aanvullende activiteiten uitgevoerd zoals een phishing campagne, toetsing op clean desk/clear screen, en een presentatie van Daniel Verlaan. Het management draagt uit dat het volgen van scholing belangrijk is. Het scholingsprogramma wordt elk jaar uitgevoerd en medewerkers nemen hier aan deel. Op dit onderdeel scoren wij 75% omdat de deelname minder hoog is dan de streefnorm van 80% van alle medewerkers.

2b iBewust handelen

Het aantal medewerkers dat voor de deadline de trainingen afrondt daalt. Het doel van het scholingsprogramma is dat medewerkers zich informatiebewust gaan gedragen. Het onderzoek dat de factoren die het effect van onze eLearning en andere interventies bepaalt is uitgevoerd. Met het resultaat van het onderzoek gaan wij binnenkort aan de slag. Op dit moment scoren wij 75% op dit punt omdat de deadline voor de deelname vaak niet gehaald wordt.

Het derde thema is **Toegangsbeveiliging**. Dit kent twee aspecten: de fysieke toegangsbeveiliging (a) tot de gebouwen en beveiligde zones binnen de gebouwen. En de digitale toegangsbeveiliging (b) tot applicaties en data. De huidige status van de fysieke beveiliging is:

3a Fysieke beveiliging

Fysieke beveiligingszones zijn ingericht en verwerkt in toegangsbeleid. Het beleid is in het afgelopen jaar tegen het licht gehouden. De score in de CyberManager is 100%

onveranderd ten opzichte van de vorige brief. Desondanks verdient de effectiviteit van het toegangsbeleid aandacht, wat ook zal gebeuren naar aanleiding van het onderzoek van afgelopen jaar.

3b Digitale beveiliging

De digitale toegangsbeveiliging is gebaseerd op de juiste omgang met accounts, wachtwoorden en multi-factor authenticatie. Het beheer van toegangsrechten betreft maatregelen die getroffen worden om ervoor te zorgen dat alleen medewerkers een account hebben, dat zij alleen toegang hebben tot de applicaties die zij nodig hebben en alleen met de juiste rechten. Om dit goed te kunnen doen moeten verantwoordelijkheden gedefinieerd zijn en de processen moeten bekend zijn bij de betrokkenen. Op het functioneren van de processen voor het toekennen van rechten aan gebruikers worden controles uitgevoerd. Dit gebeurt voor het generieke deel van het proces dat toegang geeft tot de gemeente Nijmegen omgeving. Daarnaast voor applicaties naarmate het risico hoger is. Hierbij worden nog niet alle systemen jaarlijks getoetst. De score voor dit onderdeel is 70%.

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

A.P.W. van de Klift
gemeentesecretaris

H.M.F. Bruls
burgemeester