Nijmegen

Postadres
Gemeente Nijmegen
Postbus 9105
6500 HG Nijmegen

Bezoekadres
Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactgegevens
nijmegen.nl/contact

Ons kenmerk
E26.000681

Aan de gemeenteraad van Nijmegen

Datum 26 mei 2026
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. Deze afspraak is gemaakt naar aanleiding van het rapport van de regionale rekenkamer over genaamd “Weten van je moet weten”[1]. In de brief van oktober 2025 hebben we u geïnformeerd dat we in het begrotingsproces in beeld hadden gebracht wat naar onze indruk nodig was om de eerder gestelde doelen alsnog te bereiken.[2] Inmiddels is de begroting vastgesteld en is er extra budget beschikbaar om te bouwen aan betere informatieveiligheid. Met dit budget heeft het college inmiddels het team dat aandacht besteed aan informatiebeveiliging en privacy uitgebreid. In de komende jaren volgt nog meer uitbreiding, zodat het gestelde doel om volwassenheidsniveau 3 te bereiken, gerealiseerd wordt. Dit sluit aan bij het privacybeleid en het informatiebeveiligingsbeleid. Dit houdt in dat processen voor informatiebeveiliging en privacy in de gehele organisatie gestandaardiseerd en gedocumenteerd zijn en effectief worden uitgevoerd.

In deze raadsinformatiebrief over de voortgang op informatiebeveiliging en privacy geven we inzage in de lopende ontwikkelingen. Wij beschrijven de stand van zaken van de IT-roadmap (hierna: de roadmap). Daarnaast schetsen we een totaalbeeld van de mate waarin we voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en de Baseline informatiebeveiliging overheid (BIO), de geldende privacywetgeving en het normenkader voor informatiebeveiliging bij de overheid). Dit doen we op basis van huidige versies van de normenkaders, wetend dat versie 2 van de BIO (BIO2) dit jaar geïmplementeerd wordt. Tot slot bespreken we de kritische prestatie indicatoren (KPI’s) die eerder met uw raad zijn afgestemd en later zijn bevestigd door de Auditcommissie.

---

[1] 08 2022: Regionaal rekenkameronderzoek Informatiebeveiliging en privacybescherming Nijmegen - iBabs Publieksportaal
[2] Raadsinformatiebrief ‘Voortgang op informatiebeveiliging en privacy’, 28 oktober 2025, E25.002254

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 wordt op sommige acties verder ingegaan. Deze jaarrapportage is als onderdeel van de informatie over ENSIA 2025 verstrekt. De ENSIA is de eenduidige normatiek single information audit, de manier waarop alle overheidslagen zich jaarlijks verantwoorden over hun informatiebeveiliging op basis van de BIO.

In de periode van oktober 2025 tot en met maart 2026 zijn de volgende acties afgerond:

- De verdeling van de maatregelen (die behoren bij het BIO normenkader) tussen iRvN en Gemeente Nijmegen is opgesteld
- Het geactualiseerde Informatiebeveiligingsbeleid is vastgesteld.
- De werving van de versterking van het Team Informatiebeveiliging en Privacy is compleet.
- Er is in de organisatie geoefend met casuïstiek op het gebied van rollen en verantwoordelijkheden op het vlak van iVeiligheid.
- Implementatie van een nieuw, verbeterd format voor de gegevensbeschermingseffectrapportages (data protection impact assessment, DPIA)
- Afronding van de audit over ons gebruik van politiegegevens (de Wpg-audit).

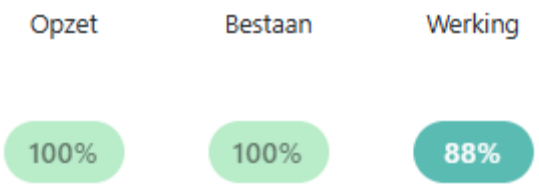
De volgende acties lopen op dit moment:

- De resultaten van de uitvraag Controlplan van de gemeentelijke functionaris voor de gegevensbescherming (FG) en chief information security officer (CISO) worden verwerkt.
- Het ontwikkelen van een eigen eLearning wordt opgestart, voor de thema's privacy, informatiebeveiliging en informatiebeheer, zodat de bewustwording van de organisatie op deze thema's verbeterd kan worden.
- Het uitvoeringsplan implementatie informatiebeveiligingsbeleid wordt uitgewerkt als onderdeel van het takenpakket van het Team Informatiebeveiliging en Privacy.
- Het BIO2 normenkader wordt geïmplementeerd in CyberManager.[3]
- Deelname aan de Pilot BIO2 implementatie VNG, met als een van de resultaten een (jaar)plan voor de implementatie van BIO2.
- Verbeteren van de privacyverklaring en het publiceren van privacyverklaringen die ingaan op specifieke thema's
- Van privacygevoelige applicaties worden autorisatie matrices opgesteld, met inachtneming van functiescheiding. Deze actie is een eind op weg en loopt in 2026 nog door.

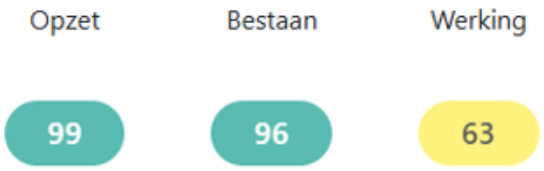
[3] De BIO2 is een vernieuwd kader voor informatiebeveiliging binnen de overheid, als opvolger van de BIO 1.04

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.
In het afgelopen jaar is het beheer op de CyberManager meer professioneel ingericht en is de herinrichting gestart.



Figuur 1 Status Informatiebeveiliging in CyberManager



Figuur 2 Status privacy in CyberManager

Informatiebeveiliging

De toetsing voor deze score is gedaan aan de hand van het BIO normenkader 1.04 omdat dit in 2025 nog van toepassing is. Daarbij 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 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.

In 2026 zal het BIO2 normenkader opgenomen worden in CyberManager. Ook zal er een eerste stand van zaken in kaart gebracht worden rond de implementatie van de relevante BIO2 maatregelen bij gemeente Nijmegen. Dit zal het startpunt vormen van het uitvoeringsplan om in de komende twee jaar de BIO2 te implementeren.

Privacy

We zien een licht stijgende trend van de mate van voldoen ten opzichte van de afgelopen raadsbrief van 28 oktober. Opzet en bestaan is nagenoeg gelijk gebleven. Hier is het, gelet

op de hogere scores, ook lastiger om winst te boeken. Bij de werking zien we een grotere sprong, van 58% naar 63%. Een stap in de goede richting, maar we zien ook dat de werking nog achterblijft. Er valt nog veel winst te behalen bij het aantoonbaar naleven van afspraken die we hebben gemaakt.

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 december 2023) 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.

Er zijn op hoofdlijnen drie aandachtsgebieden vastgesteld:

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

KPI's vanuit privacy

Gegevensbeheer is het eerste thema. Dit heeft zowel componenten van informatiebeveiliging als van privacy in zich. We delen gegevensbeheer, onderdeel privacy, op in twee onderdelen. Dat zijn DPIA's en het voldoen aan de privacy-eisen op het gebied van wetgeving en contracten.

1) 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.
Met de invoering van Borgingsmodel 3.0 van de Informatiebeveiligingsdienst, zijn er extra vereisten bijgekomen op het gebied van privacy. Hier is eerder over gecommuniceerd in de raadsbrief van oktober 2024 en maart 2025. Eén van deze extra vereisten ziet op pré-DPIA's. Dit is een vragenlijst die je invult wanneer er twijfels bestaan over of het uitvoeren van een DPIA noodzakelijk is. Bovendien is dit een handig middel om afspraken vast te leggen rondom privacyrisico's in processen waarbij een DPIA niet verplicht is. In de jaarrapportage van de FG over 2026 worden de maatregelen die volgen uit de pré-DPIA's meegenomen in de controle. Aangezien pré-DPIA's onderdeel zijn van het proces omtrent DPIA's, nemen we deze mee in deze brief.

a) Procedure pré-DPIA

Het afgelopen jaar hebben we pré-DPIA checklist ontwikkeld. Uitvoering hiervan is belegd bij de privacy officers en de FG controleert. De procedure is dus bekend en wordt gevolgd. We kunnen alleen niet garanderen dat alle processen volledig in beeld zijn. Daarom is de score 75%.

b) Resultaten uitgevoerde pré-DPIA

De uitkomsten van pré-DPIA's worden centraal opgeslagen. De maatregelen hiervoor worden meegenomen in de jaarrapportage van de FG. De score hier is daarom 100%.

c) 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.

d) 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. De score in de Cybermanager is daarom 100%.

e) 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%.

f) DPIA documenten

De score hier is ongewijzigd ten opzichte van de laatste brief en blijft dus 75%. Het feit dat dit niet 100% heeft er mee te maken dat in enkele gevallen niet alle bijlagen bij de DPIA opgeslagen zijn op dezelfde plek.

2) Privacy-eisen wetgeving en contracten

Deze KPI gaat over verwerkersovereenkomsten en andere soorten privacy-overeenkomsten (denk aan privacy protocollen en overeenkomsten onder gezamenlijke verantwoordelijkheid).

a) Overzicht convenanten bij samenwerkingsverbanden

Bij samenwerkingsverbanden maken we doorgaans aanvullende afspraken in de vorm van privacy protocollen of convenanten. Middels de jaarlijkse 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%.

b) Actueel overzicht verwerkersovereenkomsten

We hebben steeds beter overzicht van welke verwerkersovereenkomsten we allemaal hebben. Het is echter nog niet helemaal volledig. De score hier is ongewijzigd en blijft 75%.

c) Overzicht periodieke controle en bevindingen

In de jaarrapportage van de FG over 2024 zijn alle bij ons bekende verwerkersovereenkomsten op naleving getoetst. Hieruit bleek dat er nog veel verbeteringen te behalen zijn op het gebied van de naleving van afspraken uit de verwerkersovereenkomsten. De score is daarom 50%. De uitvraag over 2025 wordt nog verwerkt.

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 BIV standaard (gehanteerd binnen de informatiebeveiliging waarbij een score wordt toegekend aan het belang van beschikbaarheid, integriteit en vertrouwelijkheid) die ook door de informatiebeveiligingsdienst voor gemeenten (IBD) gebruikt wordt. Dit proces is gedocumenteerd en de resultaten zijn goedgekeurd door de eigenaren van de applicaties. De werkwijze is niet veranderd. Het aantal betrokken systemen neemt toe. Daarnaast zal het opruimen van de niet geclassificeerde informatie in het kader van Microsoft 365 nog langere tijd duren, gezien de hoeveelheid informatie en de beperkingen in capaciteit.
De score op werking is 50% omdat nog niet van alle kritieke systemen jaarlijks de classificatie opnieuw beoordeeld wordt. De cyclus van de jaarlijkse beoordeling wordt ingericht in de Cybermanager.

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 volledig 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. Dit scholingsprogramma wordt in het komende jaar herzien. Er zijn ook aanvullende activiteiten uitgevoerd zoals casusoefeningen met de managementteams en periodieke acties op het verbeteren van de wachtwoordkwaliteit. Het management draagt uit dat het volgen van scholing belangrijk is. Het scholingsprogramma is ook in 2025 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. Het gebruiken van de resultaten is nog niet gebeurd want te arbeidsintensief. Wij scoren 75% op dit punt omdat het nog niet gelukt is om verbetering te bereiken.

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% en dus onveranderd ten opzichte van de vorige brief. Desondanks verdient de effectiviteit van

het toegangsbeleid aandacht. De aanbevelingen van het onderzoek in het afgelopen jaar worden opgepakt.

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. Nog niet alle systemen worden jaarlijks getoetst. De score voor dit onderdeel is 75%.

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

A.P.W. van de Klift
gemeentesecretaris

H.M.F. Bruls
burgemeester