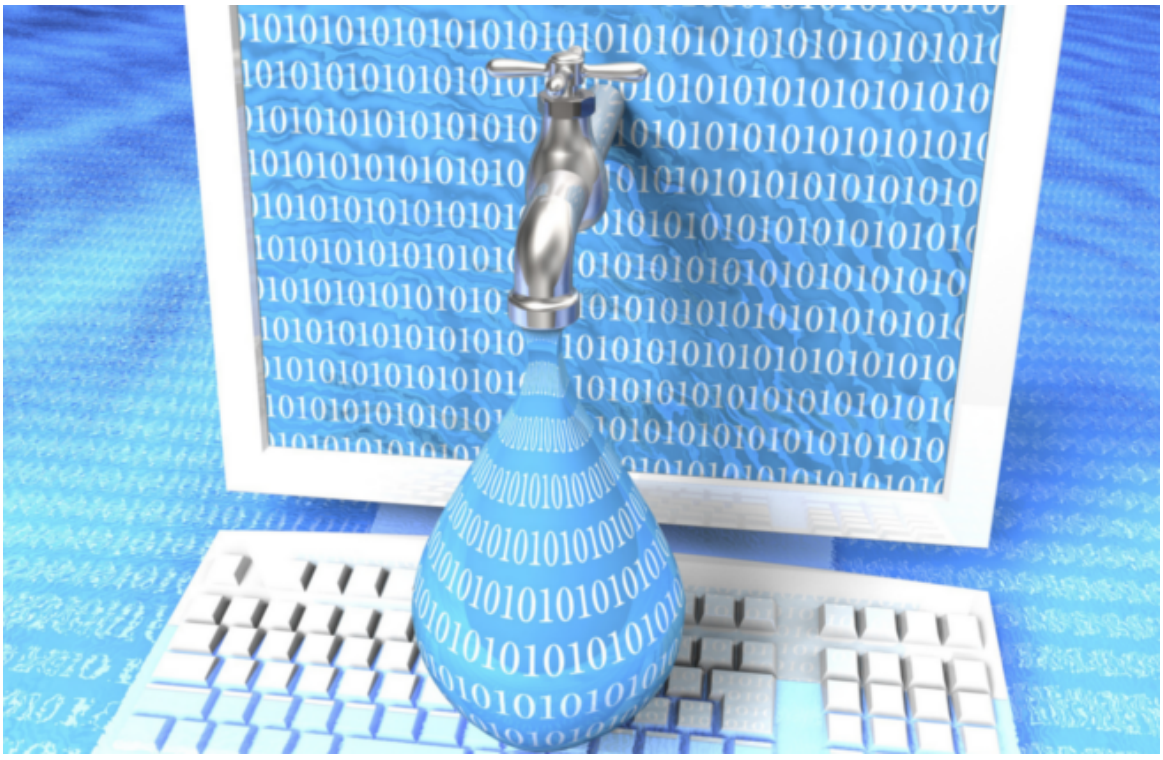
Nijmegen



Rapportage Informatiebeveiliging en Privacy 2021

CISO gemeente Nijmegen, december 2021

Informatiebeveiliging & privacy
2021

Resultaten

Beheersmaatregelen geïmplementeerd
(baseline informatieveiligheid)

Incidenten
36x

8
Data-lekken

Inzage-verzoeken burgers

Persoonsgegevens verstrekt aan derden

Verwerkersovereenkomst
(over verantwoord gebruik gegevens Nijmegenaren/ medewerkers)

Ons speelveld

Uitdagingen

Borging in processen
(incl. AVG-proof)

I-bewustzijn & scholing

Bij medewerkers
Inzet ambassadeurs

Continuïteit IT-omgeving

In de regio

Inhoudsopgave

1. Doel & wettelijk kader

Doel

In dit rapport informeren we u over de ontwikkeling van de informatiebeveiliging bij de gemeente Nijmegen. We blikken terug op het afgelopen jaar en kijken vooruit naar de ontwikkelingen in 2022 en de jaren daarna. Dit rapport is onderdeel van de regelgeving rond de Eenduidige Normatiek Single Information Audit (hierna: ENSIA).
ENSIA is een systeem van zelfevaluaties op het vlak van informatiebeveiliging. Een belangrijk document wat hieruit voortkomt is een collegeverklaring. Hiermee legt het college verantwoording af aan de raad en aan landelijke toezichthouders. De voorliggende rapportage Informatiebeveiliging en Privacy rapportage is onderdeel van onze onderbouwing bij de collegeverklaring ENSIA, waarin het college aangeeft in welke mate gemeente Nijmegen voor DigiD, Reisdocumenten, de BRP en Suwinet aan de eisen voldoet. De Chief Information Security Officer (belast met informatiebeveiliging) stelt de rapportage op, met bijdragen van de Functionaris Gegevensbescherming (belast met privacy), collega`s van control, informatiemanagement, collega`s betrokken bij informatieveiligheid en iRvN. Het rapport wordt vastgesteld door het college.

Wettelijk kader

Gemeenten hebben in de VNG-resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ uit november 2013 onder meer afgesproken dat in de jaarstukken – in het onderdeel jaarverslag - een aparte passage over informatiebeveiliging wordt opgenomen. Een periodieke rapportage aan alle managementlagen is onderdeel van de Baseline Informatiebeveiliging Overheid (BIO). Met deze passage en het onderbouwende rapport verantwoordt het college zich aan de gemeenteraad over informatiebeveiliging in brede zin.

2. Leeswijzer

Het eerste deel van dit rapport wijden we aan het schetsen van het onderwerp. Wat is het en hoe verhoudt de gemeente Nijmegen zich hiertoe. Daarna blikken we terug op het afgelopen jaar over de vooraf gestelde doelen en de behaalde resultaten. In eerste instantie voor de gemeente zelf en daarna waar het gaat om onze partners. We sluiten af met een vooruitblik naar de toekomst, het komende jaar en de langere termijn.

Ter ondersteuning vindt u voorin een infographic waarin de volgende onderwerpen zijn gevisualiseerd: 1) het speelveld waarin we ons begeven rondom het uitwisselen van gegevens, 2) de resultaten die we in 2021 boekten en 3) de uitdagingen waar we in de toekomst voor staan.

In de bijlage vindt u achtergrondinformatie over informatiebeveiliging & privacy inclusief een toelichting op veel gebruikte begrippen.

3. Ambitie

De gemeente Nijmegen wil haar volwassenheidsniveau van de informatiebeveiliging verhogen. Wij streven er naar om “in control” te zijn en daarover op professionele wijze verantwoording af te leggen, onder andere via de voorliggende rapportage. ‘In control’ betekent in dit verband dat de gemeente weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging. Daarbij weten we welke (passende) maatregelen we nemen en wie waar verantwoordelijk voor is. We zorgen voor een controleerbare planning van maatregelen die genomen moeten worden en we bewaken deze. En tot slot weten we in hoeverre de maatregelen effectief zijn en welk risico’s er over blijven.

Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is. Voor meer informatie kunt u ons informatiebeveiligingsbeleid lezen. Dit is gepubliceerd op overheid.nl.

Het team Stadscontrol binnen de gemeentelijke organisatie, met hier in ondergebracht de CISO en de FG, brengt de oordeelsvormende rol binnen de gemeente meer voor het voetlicht. Door meer aandacht te geven aan eigenaarschap, opvolging en verantwoording neemt het volwassenheidsniveau van processen toe. Risico gestuurd werken zorgt er voor dat dit zo efficiënt mogelijk wordt ingevuld.

Ook iRvN en WBRN werken aan professionalisering. Zij zijn in gesprek met een externe partij die hen naar certificering kan begeleiden. Hiermee geven zij gehoor aan de wens van gemeente Nijmegen tot meer transparantie en verantwoording ook naar hun andere partners toe.

4. Terugblik

4.1 Wat wilden we bereiken?

In 2021 is veel energie gestoken in het opvolgen van de aanbevelingen van de accountant. Het opstellen van een meerjarenplan, ambitiedocument en activiteitenoverzicht met daarin opgenomen de planning van de opvolging van alle maatregelen en aanbevelingen. De benodigde acties zijn gestart, onderweg dan wel afgerond. Er zijn acties die langer dan een jaar zullen doorlopen. De inrichting van de CyberManager heeft in 2021 een volgend stadium bereikt. Voor het verkrijgen van inzicht in de risico's die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen is het nu nodig dat de afdelingen aan de slag gaan met de risico analyses en de maatregelen implementatie.

Alle afdelingen hebben het uitvoeren van het AVG-proof plan opgepakt. Dit plan is een manier om het eigenaarschap voor het voldoen aan de privacyregels en het verbeteren van de informatiebeveiliging bij de afdelingen zelf te beleggen, zoals de BIO ook vraagt. Het in gebruik nemen van de fysieke toegangspoorten in de twee dienstgebouwen is een van deze stappen.

Om meer gestructureerd aandacht te besteden aan iBewustzijn is verplichte scholing onderdeel van de jaarlijkse plannen, naast algemene campagnes en ad hoc berichten over actuele zaken. Daarnaast wilden we in de regio aan de slag met het oefenen van het regionale ICT-crisisproces en het verbeteren van de continuïteitsplannen om beter voorbereid te zijn op een ICT crisis.

4.2 Wat hebben we bereikt?

4.2.1 De gemeente Nijmegen

Activiteiten over de hele gemeente

- Het AVG-proof project
- De Functionaris Gegevensbescherming voert gemeentebreed het controleplan uit. Het aantal uitgevoerde DPIA`s is verdubbeld.
- Het advies van iRvN met betrekking tot het gebruik van system accounts is aangenomen en wordt uitgevoerd.
- Bitwarden is als standaard wachtwoord manager beschikbaar gesteld. De uitrol bij de medewerkers loopt.
- Informatieveiligheid, Privacy en Informatiebeheer cursussen zijn beschikbaar gesteld via Studytube en voor iedere medewerker verplicht.
- De CISO's hebben regionaal een ICT-crisis oefening uitgevoerd.
- Log4j dreiging is regionaal tot dusver succesvol bestreden.
- Per 1 december is aan het team Ontwikkeling I&A een Security Officer toegevoegd ter ondersteuning van de CISO.
- Het team Stadscontrol ziet toe op het opvolgen van bevindingen en het nemen van de juiste maatregelen. Dit gebeurt door het voeren van advies gesprekken, het begeleiden van prestatie dialogen en het toetsen van maatregelen, bijvoorbeeld door het uitvoeren van audits met behulp van de CyberManager.

Een opvallende gebeurtenis in het afgelopen jaar was de discussie rond het gebruik van anonieme accounts. In Nijmegen is door de afdelingen onderzoek gedaan naar de manieren waarop anonieme accounts online gebruikt werden voor het verkrijgen van informatie op social media. Uit de verschillende werkwijzen is een protocol gedestilleerd waarin beschreven wordt hoe er verantwoord online onderzoek gedaan kan worden met gebruik van anonieme accounts. Dit protocol is vastgesteld en wordt gemeente breed gehanteerd.

Er zijn in het afgelopen jaar geen meldingen gedaan via de website van gemeente Nijmegen met gebruikmaking van de digitale klokkenluidersregeling (responsible disclosure).

Invoering van de CyberManager gaat door

De invoering van de CyberManager is nu zo ver dat implementatie taken zijn en worden uitgezet bij de afdelingen zodat zij de status aan kunnen geven van de maatregelen. Dit gaat in overleg met de afdelingen omdat hier capaciteit voor vrijgemaakt moet worden. Omdat deze stap nog niet is afgerond en de status informatie nog niet compleet is hebben we overzicht over het geheel gekregen door in de CyberManager een “interne audit” uit te voeren op de status van de BIO maatregelen. Hierbij hebben we samen met de leverancier de informatie uit de ENSIA verantwoording gebruikt en ingevoerd in de CyberManager.

In de infographic voorin kunt u zien dat in de CyberManager nu 65% van de maatregelen actief is. Dit betekent dat er over het geheel genomen weinig verschil is met het voorgaande jaar. Toch staan we niet stil. Maatregelen worden controleerbaar uitgevoerd, door de juiste verantwoordelijken. Er zijn alleen geen nieuwe maatregelen toegevoegd. Een voorbeeld hier van is toegangsbeveiliging voor het Stadhuis. Er was toegangsbeveiliging maar de Mystery Guest bezoeken toonden aan dat deze niet effectief was. Tourniquets werken beter maar leveren geen extra geïmplementeerde maatregel op. Wel kan de werking beter worden aangetoond en dit kan in de CyberManager worden opgenomen. Het beheren van de maatregelen in de CyberManager door de afdelingen zelf wordt nu ter hand genomen waarmee de waarde van de informatie in de CyberManager toe neemt.

Resultaten uit de regionale ICT-crisis oefening

In de regio is in het afgelopen jaar de opgestelde procesbeschrijving over hoe te handelen bij een informatiebeveiligingsdreiging met elkaar geoefend. Hierin zijn wij begeleid door Cuccibu. Zij hebben op ons verzoek daar een rapportage over gemaakt. De rapportage van Cuccibu schetst samengevat het volgende beeld:

- Over het algemeen hadden de deelnemers een vrij goed beeld van de procesbeschrijving en handelden zij er ook naar.
- Er is enige onduidelijkheid bij de betrokkenen over de rollen en verantwoordelijkheden van de organisaties en de betrokkenen ten opzichte van elkaar.
- Het handelingskader dat geoefend werd is een goede en belangrijke eerste aanzet om tijdens een crisis te kunnen handelen.
- Er is voor de individuele organisaties, en de overkoepelende organisatie, beleid en procedures nodig om duidelijkheid te scheppen over hoe de deelnemers in een crisis moeten handelen en hoe de communicatie plaatsvindt tussen de partijen.
- De oefening heeft aan iedereen laten zien hoe een mogelijke crisis er uit zou kunnen zien en welke acties er dan plaats moeten vinden. Alle organisaties gaan aan de slag met hun eigen en de regionale inrichting voor bedrijfscontinuiteit. Dit om de onduidelijkheden die nu nog bestaan op het vlak van rollen en verantwoordelijkheden, communicatie en escalatie, weg te nemen.
- Het is zaak om na de crisis te evalueren en aan de hand daarvan beleid, prioriteiten, producten en organisaties op elkaar af te stemmen en te waarborgen dat actie punten ook worden uitgevoerd.

IT Audit observaties van de Accountant over 2021

De jaarlijkse accountantscontrole heeft oog voor de positieve ontwikkelingen bij de gemeente. De conclusie is dat de beheersing van de geautomatiseerde omgeving verbetert en dat met name aan de implementatie kant nog verdere stappen gezet kunnen en moeten worden. De accountant adviseert capaciteit vrij te maken om de implementatie te kunnen versnellen.

De accountant is ook te spreken over de positieve ontwikkelingen in het formuleren van de verantwoordelijkheden en het eigenaarschap tussen de afdelingen van de gemeente Nijmegen. Ook de concrete stappen op het vlak van ICT-crisisbeheersing in de vorm van het oefenen van het regionale crisis proces worden positief gewaardeerd.

Wel benadrukt de accountant dat we prioriteit moeten geven aan het inzicht krijgen op de voortgang op de doelen door middel van het formuleren en meten van kritische prestatie indicatoren. Dit is ook belangrijk om ons te helpen prioriteiten te stellen voor het inzetten van capaciteit.

Resultaat uit de enquête informatiebeveiliging

In 2021 is er een enquête gehouden onder alle medewerkers van gemeente Nijmegen. De vorige enquêtes waren in 2015 en in 2016. Het doel is om deze enquête elke 2 jaar te houden zodat de ontwikkeling in de resultaten gemonitord kan worden.
Een aantal resultaten:

- Ten opzichte van de voorgaande jaren is het besef van het belang van informatiebeveiliging toegenomen (van 6,8 naar 8) maar de bekendheid met de gemeentelijke richtlijnen op dit vlak is niet gestegen.
- De omgang met wachtwoorden is verbeterd. Ze worden minder gedeeld (1% ten opzichte van 7% in het verleden) en de wachtwoorden kluis wordt meer gebruikt (19% ten opzichte van 9 % eerst)
- De meeste respondenten waren bekend met het belang van de nieuwe toegangspoorten in het Stadhuis een de Marienbeurs (69%)

Opvallend is dat in de antwoorden op de open vraag vaak aangekaart wordt dan men behoefte heeft aan meer informatie en instructie. Anderzijds is niet iedereen van plan de cursussen over informatieveiligheid, privacy en informatiebeheer te gaan volgen (50%). Daarnaast is de informatie die op het intranet geplaatst wordt vaak niet bekend (70% in het geval van de informatie over de toegangspoortjes). Op het vlak van het communiceren van informatie zullen er verbeteringen nodig zijn om er voor te zorgen dat deze scheiding tussen het aanbieden, opnemen en het toepassen van informatie verdwijnt.

Resultaat van de ENSIA Cyclus 2021

De zelfevaluatievragenlijst is gebaseerd op de BIO. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd. Door de IT-auditor is één afwijking geconstateerd die is opgenomen in een verbeterplan.

Wij rapporteren als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid, via ENSIA. Dit rapport over informatiebeveiliging en privacy is daar een onderdeel van. Vanuit de gemeentebrede zelfevaluatie wordt ook de verantwoording aan de stelselhouders bij de rijksoverheid afgeleid, de zogenaamde verticale verantwoording. Naast dit rapport zijn er ook bijlagen over DigiD, Suwinet, BRP, Reisdocumenten, BAG, BGT, BRO en WOZ bij de collegeverklaring over ENSIA. Een korte samenvatting per stelsel vindt u hier onder.

Stelsel	Samenvatting
DigiD	Strengere handhaving op normen betekent voor DigiD dat van de twintig normen per aansluiting bij twee van de vier aansluitingen er een niet voldoet. De auditor geeft wel aan dat wij elk jaar onze zaken beter op orde hebben.
Suwinet	Bij Suwinet is aan de twee toepassingen die wij al kenden er een toegevoegd. Het blijkt dat Gemeente Nijmegen verantwoordelijk is voor DKD inlezen functionaliteit zoals die gebruikt wordt door de Decos Inkomensassistent. Daarnaast is het zo dat er van de veertien normen die gelden voor de twee andere toepassingen bij er Suwinet-Inkijk een niet voldoet.
BRP	De uitslagen zijn net als vorig jaar goed. Aan de verbeterpunten bij het RNI (onderdeel van de BRP), is gewerkt (scholing, functiescheiding). Dat is positief terug te zien in de resultaten.
Reis-documenten	De uitslagen van de reisdocumenten zijn net als vorig jaar: goed. Functiescheiding wordt goed toegepast.
BAG	In 2021 zijn oppervlaktes voor woningen (en WOZ-deelobjecten) opnieuw berekend door een extern bedrijf en verwerkt in de BAG. Ten tweede heeft archiefonderzoek plaatsgevonden van verblijfsobjecten zonder woonfunctie waarbij -op het bijbehorende adres- wel bewoners staan ingeschreven in de Basisregistratie Personen en waarbij de WOZ-administratie ook een 'woning' kent. Resultaat van het onderzoek was dat de 'woonfunctie' bij een aantal verblijfsobjecten kon worden toegevoegd in de BAG. Ten derde is voldoende capaciteit geregeld bij de ODRN om inspecties ten behoeve van de BAG uit te voeren. Die inspecties worden uitgezet wanneer een terugmelding op de BAG niet met dossieronderzoek opgelost kan worden. Er is dan een verschil tussen de huidige, feitelijke situatie ten opzichte van de vergunde situatie. Bij strijdigheid met het bouwbesluit of wanneer vergunningsplichtige activiteiten zijn uitgevoerd, gaat de ODRN over tot handhaving. Bij strijdigheid met het bestemmingsplan wordt het verzoek tot handhaving door de ODRN doorgegeven aan de afdeling Ruimtelijke Planvorming. Tot slot hebben we opnieuw met 3D-techniek mutaties van en aan gebouwen gedetecteerd en worden die verwerkt in de BAG- en WOZ-registratie.
BGT	Het berichten verkeer BGT-Groen- en Wegbeheer is in productie gegaan, wat resulteerde in grote werkvoorraden aan zowel de BGT kant als de Groen- en Wegbeheer kant. Naast de mutaties in de topografie betreft het hier voor een groot deel het opknippen van groen-objecten ter plaatse van onder andere openbaar-particulier terrein. De werkvoorraad in de BGT, welke is doorgestuurd vanuit groen-beheer, is grotendeels verwerkt, maar wordt dagelijks ook weer met grote aantallen aangevuld. Van wegbeheer zullen we de komende maanden veel mutaties te verwerken krijgen. Ook hier gaat het voor een groot deel om het opknippen van in dit geval de wegobjecten. Aan de hand van controlescripts en het kwaliteitsdashboard van het Kadaster wordt de BGT verder verbeterd, wat een doorlopend proces is. De afhandeling van terugmeldingen gaat vlotter. In 2021 zijn twee meldingen niet binnen 5 dagen verwerkt. Verder zijn er veel pandmutaties verwerkt als gevolg van het BGT-BAG-WOZ/3d-mutatiedetectie project.
BRO	De BRO krijgt verder vorm. Er is een overleg geweest met de afdeling Stadsrealisatie en er is aanzet gemaakt voor een presentatie met de afdeling Stadsbeheer om m.n. het basisidee voor het verder organiseren van de BRO gerelateerde processen verder uit te dragen. De essentie is dat er per organisatorische eenheid (afdeling, bureau, thema, …) contactpersonen aangewezen worden, die kennis hebben van de BRO en zicht houden op alle binnen hun eenheid BRO-gerelateerde activiteiten. Deze contactpersonen onderhouden nauw contact met de BRO coördinator. Ze melden de projecten die op stapel staan bij deze coördinator en maken afspraken met de gegevensleveranciers, zodat gegevens conform de BRO regels worden aangeleverd. De coördinator kan voorlopig fungeren als bronhouder in het Bronhouderportaal. Dit zal later overgenomen kunnen worden door de contactpersonen of medewerkers zelf. Corona heeft wel voor vertraging gezorgd. De nieuwe registratieobjecten van tranche 3, per 1-1-21 wettelijk in werking getreden, zijn: M.b.t. Booronderzoek (3 nieuwe objecten) M.b.t. Wandonderzoek (1 nieuw object) Grondwatermonitoringnet Grondwatersamenstellingsonderzoek Grondwaterstandsonderzoek
WOZ	De BIO is volledig geïmplementeerd binnen de WOZ en er worden controles uitgevoerd op naleving.

Resultaat op het vlak van privacy

Afhandeling klachten

In 2021 zijn in totaal vier privacy-klachten bij de organisatie ingediend waar drie inmiddels formeel (gegrond) zijn afgehandeld. Bij de betreffende afdelingen waarvan de klacht gegrond is verklaard is een bewustwordingstraject gestart en zijn de betreffende procedures waar de klacht op zag herzien. Het proces rondom de afhandeling van klachten is inmiddels ondergebracht in het algemeen gemeentelijk klachtenproces waarbij de gemeentelijke klachtencoördinatoren het proces borgen. Eén klacht is rechtstreeks aan de FG-er van de gemeente Nijmegen gestuurd

Uitvoering van de plannen van aanpak 'elke afdeling privacy-proof'

Medio 2021 zijn de afdelingen begonnen om de uitvoering van de "elke afdeling AVG-proof" plannen weer op te pakken. De afdeling Zorg & Inkomen (Z&I) is de eerste afdeling waarmee begonnen is. Het traject voor Z&I liep van juli 2020 tot juli 2021. Begin 2021 is gestart met Publiekszaken en in oktober 2021 is gestart met de afdeling Stadsbeheer. Hierna volgende de andere acht afdelingen. Tijdens de uitvoering van het controlplan FG 2020 is stilgestaan bij de minimale vereisten om te voldoen aan de wet.

DPIA als continu bijstuurproces

Het instrument DPIA is momenteel nog teveel een momentopname van de privacyrisico's die spelen bij een gegevensverwerking. Ook wordt het instrument onvoldoende ingezet als monitoring op de implementatie en de borging van de ingezette maatregelen. Hier schuilt dan ook een kwetsbaarheid in. Door de ombuiging van implementatie naar beheer / controle zal de DPIA nog nadrukkelijker een onderdeel gaan vormen van de (interne) verantwoordingsplicht. In 2021 zijn in totaal elf DPIA's uitgevoerd op grote complexe gegevens verwerkingen binnen het fysiek, sociaal en veiligheidsdomein.

Naleving AVG door de organisatie

In 2021 heeft de Functionaris voor de gegevensbescherming een interne controle uitgevoerd op naleving van de AVG door de gemeentelijke organisatie. Object van onderzoek was:

- voortgang 'Mijn afdeling AVG-proof';
- registraties datalekken, klachten en incidenten zoals opgenomen in de Cybermanager;
- naleving van afspraken gemaakt in de DPIA en in de beoordelingen daarvan; en tenslotte:
- naleving van de afspraken gemaakt in verwerkersovereenkomsten (getoetst middels een steekproef van 10 overeenkomsten over de afdelingen verspreid).

Ondanks dat er grote stappen zijn gezet op het vergroten van het informatiebewustzijn en het werken conform de AVG zijn er een drietal belangrijke constateringen op te maken:

- de coronapandemie maakt het lastiger om te prioriteren op implementatie van AVG maatregelen
- de uitvoering van verwerkersovereenkomsten wordt onvoldoende getoetst op naleving bij leveranciers
- de naleving van uitgevoerde DPIA'S vindt te weinig aantoonbaar plaats.

4.2.2 iRvN

In reactie op de aanbevelingen van de accountant en gebeurtenissen als de hack van de universiteit van Maastricht is iRvN het veiligheidsproject gestart. Dit project verkeert in de afrondende fase. Een van de doelen had betrekking op het inrichten van een separaat beheernetwerk. Dit project is gepauzeerd vanwege technische problemen (Microsoft heeft het concept teruggetrokken). Om de doelen van dit project (verbeteren van de beveiliging rond beheer) toch te kunnen verwezenlijken is het project herijkt en wordt dit nu in aangepaste vorm doorgezet.
Veel maatregelen die te maken hebben met het ontdekken van problemen via het detectiesysteem (EWS) en het beheersysteem voor mobiele apparaten (MDM) zijn in 2020 ingevoerd. De implementatie heeft in 2021 gelopen en wordt in 2022 voortgezet. De aansluiting op het landelijke detectiesysteem (SIEM) kent een aantal uitdagingen. Daarom wordt onderzocht of er mogelijk alternatieven zijn. Het CSIRT dat is opgezet om informatiebeveiligingsincidenten op te pakken, functioneert goed en zal verder verbeteren met de lessons learned uit onder andere de Log4j crisis. De gemeente blijft eindverantwoordelijk en legt in die hoedanigheid ook over de bij iRvN belegde maatregelen verantwoording af via ENSIA. In deze context is iRvN vanaf 2021 begonnen met het aanleveren KPI`s die ondersteunen bij het verkrijgen van inzicht. Deze zullen in 2022 verder worden ontwikkeld.

4.2.3 Overige samenwerkingen

Afspraken met externe partijen

Om haar doelstellingen op een zo effectief en efficiënt mogelijke manier te kunnen behalen maakt de gemeente voor een aantal taken gebruik van samenwerkingsverbanden of externe relaties. Zie voor het speelveld rond gegevensuitwisseling ook de infographic. Om deze samenwerkingen tot een succes te maken worden data en informatie uitgewisseld. Dit betekent dat er afspraken gemaakt moeten worden die vastgelegd worden in dienstverleningsovereenkomsten en verwerkersovereenkomsten. Afhankelijk van de inschatting van het risico dat de gegevens lopen zullen wij waar nodig deze ‘verwerkers’ intensiever beoordelen op hun verantwoordingsplicht vanuit de AVG. Dit is met name ook een aandachtspunt van de FG. De CISO zal zich met name richten op de toetsing van de .

In het kader van het gastheerschap vult de gemeente Nijmegen voor de Meervoudige Gemeenschappelijke Regeling (MGR) en de Omgevingsdienst Rijk van Nijmegen (ODRN) een aantal maatregelen in. Het betreft maatregelen die te maken hebben met voorzieningen op het gebied van facilitair, personeel en juridische zaken. Denk daarbij aan maatregelen op het vlak van contractbeheer, toegangsbeleid en telewerken.

De ODRN en de MGR blijven verantwoordelijk en kunnen gemeente Nijmegen bevragen op de voortgang van de implementatie. Hiervoor is nog geen standaard proces afgesproken.

Midden 2018 heeft het Werkbedrijf Rijk van Nijmegen (WBRN) de beschikking gekregen over haar eigen Suwinet aansluiting. De IT-auditor geeft voor de regio gemeenten die deelnemen aan de WBRN een verklaring af over het gebruik van de Suwinet aansluiting volgens de geldende normen. Daarnaast rapporteert de WBRN in het kader van verwerkingsrelaties zoals die bijvoorbeeld geldt voor de “Doe je mee” regeling.

Op het vlak van Belastingen voert gemeente Nijmegen voor gemeente Mook en Middelaar taken uit. Over het gedeelde gebruik van de applicatie Gouw in deze context geeft de IT-auditor een verklaring af die de gemeente Mook en Middelaar in haar verantwoording gebruikt.

Ook met een partij als Samen Sterker wisselt de gemeente gevoelige gegevens uit in het kader van de uitvoering van WMO en Jeugdzorg taken. Hier over zijn convenanten afgesloten met de betrokken partijen. Over de toetsing op de uitvoering van deze convenanten is nog geen overeenstemming bereikt. Sterker heeft over 2021 4 datalekken gemeld. Dit is een verbetering ten opzichte van 2020. Zij hebben hier voor geïnvesteerd in betere training van en communicatie met medewerkers. Hierdoor worden risico`s en onduidelijke situaties eerder gesignaleerd.

5. Vooruitblik

5.1 Aanbevelingen uit externe toetsing

De externe controle door de accountant en de IT-audit in het kader van ENSIA leveren elk jaar weer aanbevelingen op die we meenemen in de ontwikkelingen van dat jaar.

IT toetsing bij de jaarrekeningcontrole

Voorafgaande aan de controle van de jaarrekening 2020 heeft de accountant onze (bedrijfs)processen beoordeeld. In een boardletter zijn deze bevindingen gerapporteerd en voorzien van aanbevelingen. De accountant ziet dat verbeteringen zijn ingezet, maar constateert dat deze nog niet volledig geïmplementeerd zijn. Hierbij adviseert hij prioriteit te geven aan de geautomatiseerde gegevensverwerking, het fundament van onze (bedrijfs)processen. Voor de accountant is deze nog niet betrouwbaar genoeg om op te kunnen steunen. Dit vergt nu nog extra controles op de gegevens uit onze financiële administratie.
Ons college heeft bij het aanbieden van de boardletter aan de raad aangeven dat “de bevindingen worden erkend en (waar nodig) passende verbetermaatregelen zullen worden ingevoerd.” Ambtelijk wordt actief hierop gestuurd en worden de bevindingen en verbeteracties drie keer per jaar geagendeerd in het Gemeentelijk Management Team (GMT).

Aanbevelingen van de accountant

In een praatplaat waarin de thema’s uit de boardletter zijn gevisualiseerd, komt IT als volgt terug.

- De accountant adviseert capaciteit vrij te maken voor het implementeren van de doelstellingen uit het meerjarenplan en het ambitiedocument.
- Rondom Cybersecurity lag de focus binnen het informatiebeveiligingsbeleid op de AVG. Hoewel dit begrijpelijk is, wordt geadviseerd om de scope te verbreden.
- Om onderbouwd te kunnen steunen op iRvN wordt aangeraden om toe te werken naar een certificering van iRvN, door een onafhankelijke partij, over de betrouwbaarheid van hun processen. Ook inzicht in en het beheersen van risico`s rond leveranciers wordt benadrukt.
- De implementatie van ‘mobile device management’ rondom het gebruik van persoonlijke apparaten wordt in 2022 uitgevoerd.
- De accountant wijst nogmaals op het belang van geprogrammeerde controles en data-analyses en deze met name ook te gebruiken in de vorm van bijvoorbeeld KPI’s bij het evalueren van de effectiviteit van het informatiebeveiligingsbeleid.

Aanbevelingen van de IT-auditor (ENSIA)

Bij de controle ten behoeve van het rapport dat de IT-auditor (2Control) afgeeft bij de collegeverklaring ENSIA zijn er dit jaar één afwijking geconstateerd die is opgenomen in een verbeterplan.

De IT-auditor formuleert een advies met betrekking tot de controle. (Dat advies moet hier nog worden ingevuld)

5.2 Komend jaar

Gezamenlijk stippelen Stadscontrol en de Informatiemanagers het groeipad uit voor de organisatie naar meer volwassenheid. Dit gebeurt op basis van de visie die de organisatie heeft op het vlak van bijvoorbeeld data gestuurd werken en het weerbaarder maken van de organisatie en de burger. Daarnaast spelen de aanbevelingen van de toetsende instanties natuurlijk ook een belangrijke rol.

In 2022 staan de volgende stappen gepland:

- Het gebruik van de CyberManager gemeente breed uitrollen
- maatregelen die volgen uit de AVG afdelingsplannen
- maatregelen op het vlak van bedrijfscontinuiteit (n.a.v. rapport Cuccibu)
- technische maatregelen uit de accountantscontrole/ENSIA
- organisatorische maatregelen in het kader van de accountantscontrole/ENSIA
- maatregelen op het vlak van de kwaliteit van data (in de context van datagestuurd werken) zullen per bron worden opgepakt.

Het informatiebeveiligingsplan van de MGR laat zien hoe zij de gemeente Nijmegen ondersteunt door het implementeren van maatregelen voor de kritische systemen en het nemen van generieke maatregelen om de IT omgeving voorspelbaarder te maken. Met name in de context van het Veiligheidsproject dat iRvN in 2021 heeft afgerond zijn een aantal acties uitgevoerd. In 2022 groeit het Veiligheidsproject door in het Hunt & Hackett project waarin een aantal maatregelen worden genomen, gebaseerd op de gap analyse die zij hebben uitgevoerd.

Het controleplan van de FG zal onder andere gevoed worden door informatie over de implementatie status van de normen zoals dat is opgebouwd in de CyberManager.

5.3 Meerjarig

5.3.1 Informatiebeveiliging

Toetsing van onszelf en onze partners wordt uitgebreid

Informatiebeveiliging en privacy vormen een essentieel onderdeel van de jaarplannen van Stadscontrol. Het ondersteunen van en bijdragen aan initiatieven op het vlak van iBewustzijn spelen een centrale rol. Denk hierbij aan een periodieke enquête van medewerkers en gesprekken met concernmanagers. In de komende jaren zullen controle mechanismen verder toegepast worden op de toetsing van informatiebeveiligingsmaatregelen, intern maar ook bij externe relaties. De verdere invoering van de CyberManager zal betekenen dat deze tool om een gemeentebreed overzicht te krijgen van de toestand van de informatiebeveiliging steeds meer sturingsinformatie zal opleveren, bijvoorbeeld voor het management van de afdelingen. Bovendien levert het de basisinformatie voor het controleplan van de FG en het ondersteunt collegiale toetsing intern maar ook bij partners in de MGR. Daarnaast faciliteert het onze eigen verantwoording richting andere partijen zoals de accountant. Op deze manier maken wij onze partners sterker en kunnen wij vertrouwen geven aan relaties die gegevens aan ons toevertrouwen, dan wel van ons afnemen.

ENSIA blijft het ijkpunt voor informatiebeveiliging

Wat de ontwikkelingen zullen zijn op het vlak van ENSIA is niet bekend. De ontwikkelingen in de stelsels zoals BIO (Baseline Informatiebeveiliging Overheid) en de DSO (Digitaal Stelsel Omgevingswet) zullen gevolgen hebben voor de toetsing. De verwachting is ook dat in de komende jaren de scope van de ENSIA audit breder zal worden, en dat er naast opzet en bestaan ook werking getoetst zal worden. De voorbereiding hier op is in 2019 bij iRvN begonnen. Op dit moment beperkt de toetsing zich formeel tot opzet en bestaan. Als de implementatie van de CyberManager is afgerond zal er ook getoetst gaan worden op werking. Toetsen op werking zal de volwassenheid van de gemeente Nijmegen ten goede komen. Een dergelijke ontwikkeling zal ook gevolgen hebben voor de eisen die wij stellen aan de partijen waar wij mee samen werken.

Contact met de Nijmegenaar verbeteren

In het contact met de burger zijn de ontwikkelingen dat er steeds meer verwacht wordt van de digitale mogelijkheden om diensten te verlenen en te communiceren. Zie bijvoorbeeld de ontwikkelingen rond manieren om je als burger te identificeren, zoals DigiD, IRMA en Eidas. Anderzijds is het zo dat er geen “one size fits all” burger is. Voor de gemeente is het van belang rekening te houden met burgers die om redenen van ongeletterdheid of geestelijke dan wel lichamelijke beperkingen, niet de mogelijkheid hebben om gebruik te maken van de digitale voorzieningen. Websites en achterliggende procedures moeten hier op onderhouden worden. Het ontstaan, dan wel vergroten, van een kloof tussen diegenen die mee kunnen komen met de ontwikkelingen en degenen die dat niet lukt moet voorkomen worden. Het bieden van alternatieve voorzieningen moet indien nodig meer aandacht krijgen om te voorkomen dat sommige burgers belemmerd worden in hun toegang tot voorzieningen en het uitoefenen van hun rechten.

5.3.2 Privacy

De uitdagingen op het terrein van privacy en informatiebeveiliging zijn ook in de komende jaren onverminderd groot. Om daarop in te spelen wordt verder ingezet op:

Van implementatie naar beheer / controle

De inrichting van de CyberManager voor informatiebeveiliging, privacy en de WPG heeft in 2021 een volgend stadium bereikt door het invoeren van normenkaders en het daaraan koppelen van maatregelen om naleving te monitoren. Voor het verkrijgen van inzicht in de risico's die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen is het nu nodig dat de afdelingen zelf aan de slag gaan met de risico analyses en de implementatie van maatregelen.

De check op de "in control-maatregelen" (= de onderdelen van het controlplan) willen we als volgt invullen:

- Via het systeem Cybermanager kunnen we zien welke maatregelen getroffen zijn en welke nog niet. Hier kan een actie uit voortkomen. Dit betreft informatie die voorradig is in het systeem (werkwijze: check melding in systeem en opvolging daarvan).
- Via gerichte vragen kunnen we nagaan of met name 'nalevingen' plaatsvinden i.c. wordt ook datgene gedaan wat we afgesproken hebben. Dit gaat met name over houding en gedrag. Deze vragen worden aan de afdelingshoofden - als gegevensverantwoordelijke – gesteld (medium = vragenlijst).

Tenslotte gaan we via gerichte steekproeven "checken" wat de kwaliteit van maatregelen is.

Het is noodzakelijk het komend jaar verder aan de slag te gaan met de ingezette lijn. Dat betekent dat de volgende stappen staan gepland:

- Het gebruik van de CyberManager verder uitrollen;
- maatregelen die volgen uit de AVG afdelingsplannen op basis van het project "mijn afdeling AVG proof";
- maatregelen op het vlak van de kwaliteit van data (in de context van datagestuurd werken) zullen per bron worden opgepakt;
- Implementeren van de aanbevelingen van de Functionaris voor de gegevensbescherming op basis van het uitgevoerde controleplan over 2021 (denk aan proces aanpassingen in leveranciers management)
- Het sturen op 'spontane naleving'. Dat wil zeggen dat de aspecten (zoals kennis en kunde, kosten/baten, mate van acceptatie etc.) ten behoeve van spontane naleving terugkomen in de aansturing van medewerkers; denk aan afspraken rond opleiding.

Bewustwording en weerbaarheid

Op het gebied van bewustwording heeft in 2019 een 'Mystery visit' plaatsgevonden. Hier zijn een aantal verbeterpunten uit naar voren gekomen. Die hebben wij in 2020 en 2021 geïmplementeerd. Dit heeft onder andere geleid tot een voorstel tot het benoemen van i-bewustzijn als belangrijk thema voor de Nijmegen School in 2021. In de digitale opleidingsmodule zijn verplichte leerlijnen opgenomen over Privacy en Informatiebeveiliging opgenomen voor alle medewerkers. Ook heeft in 2021 een phishingactie plaatsgevonden. De uitkomsten van deze actie worden meegenomen in het opleidingsprogramma. Dit heeft (mede) geleid tot de implementatie van een wachtwoordmanager en mobile device management.

Bijlage: achtergrond & begrippen

Wat is Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor een pakket aan maatregelen, die getroffen worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te garanderen, en te beschermen tegen bedreigingen. Het begrip 'informatiebeveiliging' heeft te maken met:

- *beschikbaarheid / continuïteit*: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid:* het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

  Er is ook een sterke samenhang met de archiefwet. In het Informatiebeveiligingsbeleid van gemeente Nijmegen wordt daarom in deze context ook verwezen naar duurzame opslag:
- *duurzaamheid:* het zorg dragen voor de tijdige archivering van informatie zodat ook in de toekomst verantwoording en geschiedschrijving mogelijk blijft. Dit aspect komt voort uit de archiefwet.

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie is essentieel voor een gemeente. Gemeente Nijmegen wil zich verantwoordelijk gedragen, aanspreekbaar en servicegericht zijn. Gemeente Nijmegen wil bovenal transparant en proactief verantwoording afleggen aan burgers en raadsleden en met minimale middelen maximale resultaten behalen. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

Wat is Privacy

De Algemene Verordening Gegevensbescherming (AVG), is mei 2018 van kracht geworden. Er is in 2017 een Functionaris Gegevensbescherming (FG) aangesteld alsook een Privacy Officer (PO). Het Privacy beleid van gemeente Nijmegen legt de nadruk op:

- Transparantie en communicatie
- Ethiek en minimalisatie
- Privacy by Design
- Rechten van de betrokkene
- Relatie met informatieveiligheid

Wat zijn de kaders & hoe toetsen we daarop?

De AVG spreekt van het beschermen van persoonsgegevens met afdoende technische en organisatorische maatregelen. De BIO is het normenkader dat voor een gemeente (overheid) bepaalt of technische en organisatorische maatregelen afdoende zijn.

De standaard voor het toetsen van deze normen kaders is geformuleerd door de beroepsvereniging van register auditors in Nederland, de NOREA.

Deze normenkaders en de toetsing van de toepassing daarvan door middel van de vragen die geformuleerd zijn door de NOREA zijn de basis voor de inhoud van ISMS en PIMS systemen zoals de CyberManager die door gemeente Nijmegen gebruikt wordt.

Waar liggen de bevoegdheden?

De functie van CISO is verplicht gesteld via de BIO. De CISO is verantwoordelijk voor het beveiligen van de informatie om in de beschikbaarheid, integriteit en vertrouwelijkheid te kunnen voorzien die nodig is voor de dienstverlening. De CISO heeft een derdelijns toetsende rol maar geeft ook advies.

De functie van FG is verplicht gesteld (voor een gemeente) via de AVG. Is verantwoordelijk voor de bescherming van de privacy van burgers en medewerkers van gemeente Nijmegen. Het accent van de derdelijns FG rol ligt meer op toetsing en minder bij advies.

In het normenkader van de BIO is het College van B&W eindverantwoordelijk voor de risico`s die aanvaard worden en de maatregelen die getroffen worden. Deze verantwoordelijkheid begint bij de eigenaren in de lijn die voor hun processen bepalen welke keuzes zij willen maken bij het bereiken van hun doelen. Aangezien het college van B&W eindverantwoordelijk is zijn zij de enige die risico`s kunnen accepteren.

Afkortingen

Afkorting	Uitleg
AVG	Algemene Verordening Gegevensbescherming. In werking getreden op 25 mei 2018. Sinds dat moment geldt in de gehele Europese Unie dezelfde privacywetgeving.
BAG	Basisregistratie Adressen en Gebouwen bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente.
BGT	Basisregistratie Grootschalige Topografie is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd.
BIO	Baseline Informatiebeveiliging Overheid. Van kracht sinds 1 januari 2020. Een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid gebaseerd op de internationaal erkende en actuele ISO-normatiek.
BRO	Basisregistratie Ondergrond bevat gegevens over geologische en bodemkundige opbouw van de Nederlandse ondergrond.
BRP	Basisregistratie Personen bevat persoonsgegevens van inwoners van Nederland en van personen die Nederland hebben verlaten
CISO	Chief Information Security Officer verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan
CMM	Capability Maturity Model. Amerikaans model dat gebruikt wordt om het stadium van volwassenheid van een proces (organisatie) uit te drukken.
DigiD	Digitale Identiteit s een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren, een soort digitaal paspoort voor overheidsinstanties.
DKD	Digitaal Klantdossier gegevens die ingelezen kunnen worden vanaf het Inlichtingenbureau met betrekking tot werk en inkomen.
DPIA	Data Protection Impact Assessement oftewel gegevensbeschermingseffectbeoordeling is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
ENSIA	Eenduidige Normatiek Single Information Audit heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door toezicht te bundelen en aan te sluiten op de gemeentelijke P&C cyclus
EWS	Early Warning System. Systeem voor het analyseren van log informatie en het voeden van het SIEM systeem

Afkorting	Uitleg
FG	Functionaris voor de Gegevensbescherming is een onafhankelijke deskundige op het gebied van gegevensbescherming die binnen een organisatie (of een aantal organisaties) wordt aangewezen om te adviseren, informeren en toezicht te houden op de naleving van de AVG.
ISMS	Information Security Management System is een verzameling van alle (onderling gerelateerde) informatiebeveiligingselementen van een organisatie die ervoor moet zorgen dat beleid, procedures en doelstellingen samenhangend kunnen worden gecreëerd, geïmplementeerd, gecommuniceerd en geëvalueerd om de algehele veiligheid van de informatie van een organisatie beter te garanderen.
MDM	Mobile device management. Het (op afstand) beheren van mobiele apparaten zoals laptops, smartphones en tablets.
NOREA	Nederlandse Orde van Register EDP-Auditors is de beroepsorganisatie van IT-auditors in Nederland.
PIMS	Privacy Information Management System ondersteunt in het managen van een aantal registraties (Datalekken, Verwerkingsregister, Data Protection Impact Assessments (DPIAs), Risico's, Maatregelen, Verzoeken, Toestemmingen) om AVG compliant te zijn.
PO	Privacy Officer is degene die de eerste lijn van advies dient, tot op casus niveau, op het vlak van privacy en het voldoen aan de AVG.
RMC	Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten richt zich op jongeren tussen 18 en 23 jaar, met het doel voorwaarden te scheppen zodat zij een passende onderwijs- en/of arbeidsmarktpositie kunnen bereiken.
SIEM	Security Incident and Event Monitoring. Systeem voor het analyseren van log informatie vanuit verschillende gemeenten zodat informatie over gebeurtenissen snel gedeeld kan worden.
SUWI	Wet Structuur Uitvoering Werk en Inkomen. Suwinet is de elektronische infrastructuur gebruikt voor de uitvoering van de taken in het kader van de wet SUWI, en sommige ook niet-SUWI taken.