



Nijmegen

Bits of Freedom
t.a.v. mevrouw N. Benaissa
Prinseneiland 97h5
1013 LN AMSTERDAM

Datum 28 september 2021
Onderwerp Wob-verzoek inzake voortgang naleving
AVG

Geachte mevrouw Benaissa,

Op 9 september 2021 stuurde u een brief. Daarin vraagt u op grond van de Wet openbaarheid van bestuur (Wob) om de rapportages die zijn opgesteld inzake de evaluatie van de AVG en Informatiebeveiliging over de periode 2017 tot heden. Alsmede de bestuurlijke en ambtelijke reacties daarop.

Uw Wob-verzoek:

Wij zijn verplicht bij een Wob-verzoek informatie openbaar te maken als aan de volgende voorwaarden is voldaan:

- De informatie is ergens vastgelegd, op papier, in een computerbestand of op wat voor gegevensdrager ook.
- De gemeente beschikt over de informatie.
- De informatie gaat over een bestuurlijke aangelegenheid, dat wil zeggen over beleid van gemeente Nijmegen, inclusief de voorbereiding en uitvoering ervan.

De door u gevraagde documenten zijn meegestuurd met deze brief. Dit behoudens de ambtelijke reacties welke zijn gebaseerd op persoonlijke beleidsopvattingen.

Als u het niet eens bent met dit besluit, kunt u een bezwaarschrift indienen bij het college van Burgemeester van Nijmegen. Het adres is:

Burgemeester van Nijmegen
Postbus 9105
6500 HG NIJMEGEN

Zorgt u ervoor dat u het bezwaarschrift indient binnen zes weken na de dag waarop deze brief is verstuurd. Daarmee voorkomt u dat wij uw bezwaarschrift niet meer kunnen behandelen omdat u het te laat indient. Het bezwaarschrift bevat ten minste:

- uw naam, adres en handtekening;
- de datum waarop u uw bezwaarschrift schrijft;

Postadres

Gemeente Nijmegen
JZ10
Postbus 9105
6500 HG Nijmegen

Bezoekadres

Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactpersoon

Niels de Jager
n.de.jager@nijmegen.nl
T 024 - 329 20 12

Ons kenmerk

D211181433

Bijlage(n)

Bijgevoegd: Ja

- een omschrijving van het besluit waar u het niet eens mee bent (u kunt bijvoorbeeld datum en kenmerk van deze brief vermelden of een kopie meesturen);
- de reden waarom u het niet eens bent met dit besluit.

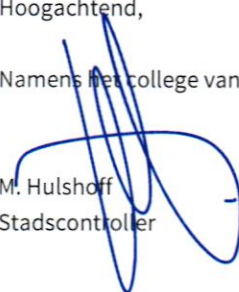
Het is mogelijk om uw bezwaarschrift digitaal in te dienen via een webformulier in de digitale balie van de gemeente Nijmegen (nijmegen.nl). Voor het indienen van een digitaal bezwaarschrift dient u in het bezit te zijn van een DigiD.

Tenslotte geeft u in het Wob verzoek aan dat u graag met de gemeente Nijmegen in gesprek wilt gaan over de uitdagingen, werking, en naleving van de Algemene verordening gegevensbescherming binnen de gemeente Nijmegen. Voor een afspraak hierover kunt u contact opnemen met de gemeentelijke Privacy Officer, de heer N. de Jager. De contactgegevens treft u hierboven aan.

Hoogachtend,

Namens het college van burgemeester en wethouders.

M. Hulshoff
Stadscontroller



Aan

De Burgemeester
Wethouder Helmer

Registratienummer / datum

1 september 2019

Opgesteld door, telefoonnummer

N. de Jager, 20 12
Rob Sijm, 9650

Visie vooraf

Jan de Roos
Kenniscuster Privacy en Informatiebeveiliging

Extra afschriften voor

Onderwerp

Evaluatie Privacybeleid 2018

Geachte Burgemeester, Geachte wethouder Helmer,

Vorig jaar juni heeft het college het privacybeleid 2018 vastgesteld. Onderdeel van de besluitvorming betrof het jaarlijks evalueren van het beleid.

Implementatie

Afgelopen jaar is enerzijds ingestoken op implementatie van de verplichtingen vanuit de AVG en anderzijds op het intern inrichten van de organisatie op het gebied van Privacy. Zo is het kenniscuster Privacy en Informatiebeveiliging opgericht en is een kennispagina op intranet ingericht. Ook is een portal op onze website ingericht waar geclusterd alle informatie met betrekking tot de privacywetgeving is terug te vinden.

Rechten van betrokkenen

Met de invoering van de AVG zijn de rechten voor burgers in het kader van de bescherming van de privacy versterkt. Dit betreft onder andere het recht op inzage in de verwerking van de eigen persoonsgegevens. Hierop is vroegtijdig geanticipeerd door het opzetten van een werkproces. Door dit werkproces zijn wij in staat om inzageverzoeken proportioneel af te handelen in relatie tot de belasting op de ambtelijke organisatie. Het afgelopen jaar hebben wij 29 verschillende inzageverzoeken afgehandeld.

Klachten

In het afgelopen jaar heeft het vigerende privacybeleid niet tot concrete aanpassingsverzoeken geleid. Dit noch vanuit de organisatie of vanuit burgers. In de periode juni 2018 t/m mei 2019 zijn er in totaal acht klachten door burgers ingediend. In drie gevallen zijn de klachten gegrond verklaard. In twee van de klachten was sprake van het -zonder informeren van de betrokkene- doorzenden van gegevens aan een derde partij. Bij de betreffende afdelingen is een bewustwordingstraject gestart en zijn de betreffende procedures herzien. Bij de derde klacht was sprake van het zonder toestemming van de betrokkenen publiceren van foto's van minderjarige in een beleidsdocument.

Eigenaarschap

In februari 2019 is eigenaarschap op i-bewustzijn belegd bij de afdelingen. Hierdoor is het afdelingshoofd verantwoordelijk - op organisatieniveau- voor de verwerking van persoonsgegevens binnen de betreffende afdeling. Geconstateerd kan worden dat hierdoor op afdelingen bewustwording op de AVG in relatie tot het privacybeleid toeneemt. Afdelingen zijn gestart met het opstellen van een plan van aanpak op I-bewustzijn en worden hierdoor ook gedwongen om kritisch te kijken naar de huidige werkprocessen.

Privacy ambassadeurs

Binnen elke afdeling is naast het benoemen van eigenaarschap ook een privacy ambassadeur aangewezen. Dit is een medewerker binnen de afdeling die inhoudelijk op de hoogte is van de werkprocessen maar ook affiniteit heeft met de aspecten van de privacywetgeving.

Partners en gemeenschappelijke regelingen

Met de invoering van de AVG is ook gekeken naar de rol en verantwoordelijkheden van onze partners. Het veilig en rechtmatig verwerken van persoonsgegevens door onze partners straalt namelijk ook uit op ons. Gelet hierop hebben wij bij alle partners de rollen en posities in het kader van de AVG vastgesteld. Samen met de partners zijn samenwerking- en verwerkersovereenkomsten gesloten en zijn gegevensuitwisselingen waar mogelijk geanalyseerd. Tevens is gemeente breed gestart met een inhaalslang op het afsluiten of actualiseren van verwerkersovereenkomsten. Verwerkers die onder verantwoordelijkheid van de gemeente Nijmegen gegevens verwerken gaan wij risicogestuurd en waar nodig intensiever beoordelen op hun verantwoordingsplicht vanuit de AVG.

Praktijk

Het privacybeleid omarmt de uitgangspunten van het manifest 'Open & Weerbaar'. Een van de belangrijkste uitgangspunten van het beleid betreft het rechtmatig verwerken van persoonsgegevens. Het streven van Nijmegen is het ethisch (willen wij dit?) en rechtmatig (mogen wij dit?) verwerken van persoonsgegevens. Daarnaast maken wij gebruik van de wettelijke mogelijkheden ter voorkoming van maatschappelijke onrust.

In de praktijk blijkt dat bij specifieke gegevensverwerkingen binnen het sociaal- en veiligheidsdomein incidenteel discussies ontstaan over de rechtmatigheid van de betreffende gegevensverwerking. Soms heeft dit te maken met het feit dat niet altijd duidelijk is wat de rechtmatige basis vormt voor de uitvoer van het specifieke werkproces (taakstelling vs. rechtmatigheid). Twee concrete gegevensverwerkingen; het versturen van persoonsgebonden brieven in het kader van Boekstart en Schoolwijzer zijn om deze reden beëindigd. Naar aanleiding van deze klachten is tevens het proces tot gegevensverwerkingen met de BRP als gegevensbron herzien.

Het afgelopen jaar is door de landelijke media veel aandacht geschonken aan de handhaving van de nieuwe privacywetgeving. De angst op hoge boetes die hierdoor is ontstaan heeft zich incidenteel omgezet naar een kramp op de werkvloer. De bijkomstige onduidelijkheid van de interpretatie van sommige bepalingen uit de AVG maakt het dat soms keuzes worden gemaakt om risico vermijdend te werken. Door middel van het sturen op bewustwording proberen wij afdelingen de juiste keuzes te laten maken. Door het uitblijven van jurisprudentie en concrete adviezen van de Autoriteit Persoonsgegevens varen wij vooralsnog op ons eigen kompas en zoeken waar nodig en passend contact met andere gemeenten.

Privacy by design

Het afgelopen jaar is kritisch gekeken naar de borging en uitwerking van Privacy by design. In samenspraak met de Radboud Universiteit zijn acht strategieën opgesteld waar nieuwe gegevensverwerkingen aan moeten voldoen. Deze strategieën zijn omgezet naar concrete eisen en wensen en zijn ingebed in het inkoopproces en bij de

Memorandum

afdeling I&A. Leveranciers omarmen de uitgangspunten. De praktijk blijkt weerbarstiger; leveranciers vinden het lastig om in technisch opzicht aan de uitgangspunten te kunnen (of willen) voldoen. Wel zien wij een verbetering van het bewustzijn op dit onderwerp.

Bewustwording

Onderdeel van de implementatie van de AVG betreft het creëren van bewustwording onder de medewerkers. Daartoe ondernemen wij gemeentebreed bewustwordingsactiviteiten (voorlichting, mystery guest, usb-sticks) als ook wordt door de afdelingshoofden in beeld gebracht wat nodig is om het bewustzijn onder medewerkers te verhogen. Op plekken waar de urgentie het hoogst is, gelet op organisatorische kwetsbaarheden versus de mate van vertrouwelijkheid van gegevensverwerkingen, wordt geprioriteerd. De menselijke factor blijft de grootste kwetsbaarheid. Het vinden van een evenwicht van de omvang van investering die je doet in termen van tijd, cultuur, capaciteit en geld versus het effect cq. de bereidheid om bewust risico's te lopen, blijft een constant aandachtspunt.

De komende periode

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

- **Voorlichting en advies;** een actuele vraag is hoe vanuit professie om te gaan met het gebruik van social media kanalen zoals Whatsapp en Facebook. **Van opzet naar werking;** inmiddels zijn de nodige slagen gemaakt om in de opzet eigenaarschap te organiseren rondom privacy en informatiebeveiliging. Na de opzet komt nu de praktijk aan bod. In de praktijk dient namelijk te blijken dat de afdelingshoofden zorg dragen voor benodigde technische en organisatorische maatregelen om de vertrouwelijkheid van gegevensverwerkingen te kunnen garanderen. Daarin is de ene afdeling mede vanuit hun oorsprong, verder dan de andere afdeling.
- **Continu proces;** in het kader van risicomanagement willen wij een stevig aandachtspunt vestigen op de doorontwikkeling van het instrumentarium Data Privacy Impact Assessment (DPIA). Wij zijn ons ervan bewust dat het instrument DPIA momenteel een momentopname is van de privacyrisico's die spelen bij een gegevensverwerking. Aan een keer uitgevoerde DPIA wordt momenteel geen follow-up gegeven. Hier schuilt dan ook een kwetsbaarheid in. Tevens is het lastig om hierdoor te voldoen aan de verantwoordingsplicht.
- **Leren van wat wij doen;** zoals bij elk thema gaan er ook wel eens dingen verkeerd, bijvoorbeeld een datalek, het is de kunst daar een leermoment van te maken. Juist door het leren van onze ervaringen ontstaat de mogelijkheid om beter te worden. Het breder uitdragen van deze geleerde lessen kan helpen in de bewustwording en daarmee weerbaarder maken van medewerkers en bestuurders.

Natuurlijk blijft er altijd iets te wensen als het gaat over de mate waarin wij onze privacy en informatiebeveiliging op orde hebben. Daar werken wij dagelijks aan. Wij kunnen niet voorkomen dat er op het terrein van gegevensverwerkingen zaken verkeerd kunnen gaan, wel kunnen we streven naar een situatie waarin de organisatie meer bewust en weerbaarder wordt op het terrein van privacy en informatiebeveiliging.

Advies

Wij stellen voor om op dit moment geen wijziging aan te brengen in het privacybeleid en het huidige beleidsstuk te continueren. Tevens om vanaf heden de evaluatie van het privacybeleid integraal mee te nemen in de jaarlijkse evaluatie van het Informatiebeveiligingsbeleid. Dit gelet op de onderlinge samenhang van de twee thema's. Deze evaluatie zal met inbegrip van de hiervoor genoemde evaluatie punten medio september aan het college worden aangeboden.

Jaarrapportage Privacy 2020

Versie 0.4. 23/11/20/PK/NdJ/EZ

Inleiding

Elke organisatie heeft een verantwoordingsplicht als het gaat om het omgaan met privacy. Deze jaarrapportage is een invulling van onze verantwoordingsplicht, waarin wij samen optrekken met de CISO in het ENSIA verantwoordingstraject. Tevens geeft deze rapportage een invulling aan de verantwoordingsplicht vanuit de AVG.

Op het gebied van ICT-control (CISO) en privacy (Functionaris Gegevensbescherming) heeft Stadscontrol een specifieke taak. De uitdagingen op het terrein van privacy en informatiebeveiliging zijn onverminderd groot en de beantwoording hiervan vormt een continu proces. In dit kader zullen er verdere maatregelen worden ingevoerd op het vlak van efficiënte, verantwoording, duurzaam digitaal informatiebeheer, transparantie over het werken met persoonsgegevens en het duurzaam borgen van privacy bewustzijn binnen de gemeentelijke organisatie. In onderstaande paragrafen (gebaseerd op de inhoud van de AVG) gaan we inhoudelijk nader in op voortgang en resultaten in 2020 (en voor zover nodig voor nader inzicht of ontwikkeling; ook jaarschijf 2019).

Rechten van betrokkenen

Burgers hebben op basis van de Algemene verordening gegevensbescherming (verder: AVG) een aantal rechten waar gebruik van kan worden gemaakt. Dit betreft onder andere het recht op inzage in de verwerking van de eigen persoonsgegevens. Dit ter controle van de juistheid en rechtmatigheid ervan. Hiervoor is een gemeentebreed proces ingericht wat tevens is gekoppeld aan de partners die in onze opdracht persoonsgegevens verwerken. Door dit werkproces zijn wij in staat om inzageverzoeken proportioneel en tijdig af te handelen in relatie tot de belasting op de ambtelijke organisatie. In 2019 hebben wij 39 verschillende inzageverzoeken afgehandeld. Over 2020 zijn het er tot nu toe 30. Ook op dit proces “leren wij door te doen”. Zo zijn wij vanuit Legal Valley¹ (Juridisch Kennisnetwerk) met inzet van Legal Tech (automatiseren van juridische processen) aan het onderzoeken of dit proces verder geoptimaliseerd en vereenvoudigd kan worden.

Afhandeling Klachten

In het afgelopen jaar heeft de evaluatie van het privacybeleid niet tot concrete aanpassingsverzoeken geleid. In de periode januari 2020 tot heden zijn er in totaal vier klachten door burgers ingediend. In twee gevallen zijn de klachten gegrond verklaard. 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.

Uitvoering van de plannen van aanpak ‘elke afdeling privacy-proof’

In 2019 heeft elke afdeling een scan gemaakt in hoeverre de afdeling voldoet aan de AVG. Dit heeft geleid tot een plan van aanpak per afdeling. In februari 2020 is het voorstel: “elke afdeling AVG-proof” vastgesteld. Hiermee worden alle afdelingen op termijn AVG volledig proof gemaakt. De afdeling Zorg & Inkomen (Z&I) is de eerste afdeling waarmee begonnen is. Het traject voor Z&I loopt van juli 2020 tot juli 2021. Hierna volgende de andere 13 afdelingen. Dit betekent niet dat de betreffende afdelingen in de uitvoering van hun werk niet hoeven te

¹ <https://legalvalleynederland.nl/>

voldoen aan de wettelijke voorschriften op het gebied van privacy. De functionaris voor Gegevensbescherming monitort dit ook actief.

Inrichting en uitvoering controleplan

Om in control te zijn op het gebied van privacy dienen een aantal verplichte maatregelen genomen te worden. Deze zijn: Verwerkingsregister bijhouden; data protection impact assessment (DPIA) uitvoeren; Register bijhouden van datalekken; Aantonen toestemming betrokkenen voor gegevensverwerking; Aanstellen functionaris gegevensbescherming (FG). Deze verplichte maatregelen zijn inmiddels allemaal ingevoerd.

Tevens adviseert de AP om extra maatregelen te nemen:

Bij een gedragscode aansluiten: O&S sluit daarbij aan (landelijke code ligt bij AP).

Een certificaat behalen: wij voldoen aan de BIO (ISO 27001).

Een specifiek ICT-beveiligingsbeleid hanteren: deze is bestuurlijk vastgesteld.

Verantwoording afleggen in het gemeentelijk jaarverslag: dit is onderdeel van de jaarrekening.

Van implementatie naar beheer / controle

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 (werkwijze: een paar vooraf aangekondigde steekproeven).

DPIA als continu bijstuurproces

In het kader van risicomanagement voeren wij Data Privacy Impact Assessment (DPIA) uit op nieuwe en bestaande gegevensverwerkingen. Wij zijn ons ervan bewust dat het instrument DPIA momenteel nog teveel een momentopname is van de privacyrisico's die spelen bij een gegevensverwerking. Wij constateren namelijk dat afdelingen die een DPIA hebben uitgevoerd dit nog niet gebruiken als terugkerend evaluatie-instrument bij proceswijzigingen. 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 2019 en 2020 zijn in totaal negen DPIA's uitgevoerd op grote complexe gegevensverwerkingen binnen het fysiek, sociaal en veiligheidsdomein.

Bewustwording en weerbaarheid

Op het gebied van bewustwording heeft in 2019 een ‘Mystery visit’ plaatsgevonden. Hierbij is door een onafhankelijk bureau onderzoek uitgevoerd naar onze fysieke basisbeveiliging en de wijze waarop medewerkers omgaan met privacygevoelige informatie. Hier zijn een aantal verbeterpunten uit naar voren gekomen. Die wij nu in 2020 implementeren. Dit heeft onder andere geleid tot een voorstel tot het benoemen van i-bewustzijn als belangrijk thema voor de Nijmegen School in 2021. Ook heeft in 2020 een phissingactie plaatsgevonden. De uitkomsten van deze actie worden meegenomen in het i-bewustzijn. Ook heeft dit geleid tot de implementatie van een wachtwoordmanager en mobile device management.



Nijmegen

Besluitenlijst Collegevergadering

Datum 13-04-2021
Tijd 9:00 - 12:30
Locatie SH b0.02/b0.03

Aanwezigen

Voorzitter H. Bruls
Wethouders M. Esselbrugge, P. Molenaar, H. Tiemens, B. Velthuis, N. Vergunst en G. Visser
Gemeentesecretaris A. van Hout
Communicatie S. Bronkhorst
Notulist M. Sofovic

Aldus vastgesteld in de vergadering van:
20 april 2021

De voorzitter

De secretaris

3.0 Vaststellen bespreekvoorstellen

3.1 Actieplan voor de binnenstad

Besluit

Advies

1. Het Actieplan voor de binnenstad vast te stellen.
2. De stadscentrummonitor 2020/2021 vast te stellen.
3. Verbijzondering van het investeringskrediet K000333 over te hevelen naar I003343 zodat de acties uit het actieplan kunnen worden uitgevoerd.
4. Begrotingswijziging BW-01782 waarmee de verbijzondering verwerkt kan worden in de begroting, vast te stellen.
5. De brief aan de raad over de actieplan vast te stellen.

3.2 Programma van eisen nieuwe woonwagenstandplaatsen

Besluit

1. Het programma van eisen voor de nieuwe woonwagenstandplaatsen als onderdeel van de QuickScan naar woonwagenlocaties, vast te stellen.
2. De brief aan de raad over het programma van eisen voor nieuwe woonwagenstrandplaatsen vast te stellen.

4.0 Vaststellen conformvoorstellen

4.1 Raadsinformatiebrief uitwerking Erfgoedstrategie

Besluit

1. De brief aan de raad over de uitvoering van de Erfgoedstrategie vast te stellen.

4.2 Verklaring inzake informatiebeveiliging DigiD en Suwinet ten behoeve van ENSIA 2020

Besluit

1. De collegeverklaring informatiebeveiliging DigiD en Suwinet vast te stellen, waarin wij verklaren dat bij gemeente Nijmegen op 31 december 2020 de interne beheersingsmaatregelen in opzet en bestaan nagenoeg voldoen aan de geselecteerde normen inzake DigiD en Suwinet, met uitzondering van de elementen DigiD U/WA.05, U/PW.03 en C.04, Suwinet DKD-Inlezen en 9.2.5 (voor het onderdeel Inkijk).
2. De Letter of Representation ENSIA Nijmegen 2020 vast te stellen, waarmee wij bevestigingen aan de auditor 2-Control afgeven.
3. De verantwoordingsrapportage Beheer en Bestuur Basisregistratie Adressen en Gebouwen 2020 vast te stellen.
4. De verantwoordingsrapportage Beheer en Bestuur Basisregistratie Grootchalige Topografie 2020 vast te stellen.
5. De verantwoordingsrapportage Basisregistratie Ondergrond 2020 vast te stellen.
6. Het Verbeterplan ENSIA 2020 voor kennisgeving aan te nemen.
7. De brief terugkoppeling ENSIA BAG 2019 zelfevaluatie voor kennisgeving aan te nemen.
8. De Rapportage Informatiebeveiliging en Privacy 2020 voor kennisgeving aan te nemen.
9. De brief aan de gemeenteraad over ENSIA 2020 en de Rapportage Informatiebeveiliging en Privacy 2020 vast te stellen.

**4.3 Mandaat verlening aanvragen op grond van artikel 10 e.v. Wet explosieven
civiel gebruik**

Besluit

1. Mandaat te verlenen aan de procesmanager Veiligheid voor de beoordeling van en besluitvorming op aanvragen op grond van artikel 10 e.v. van de Wet explosieven civiel gebruik (Wecg). Dit mandaat ziet op de aanvragen door Brown and Mason voor vergunningen op grond van artikel 10 e.v. Wecg voor de overbrenging van explosieven ten behoeve van de sloopwerkzaamheden op de locatie Engie Energie Nijmegen N.V., Hollandiaweg , 6541 BL, te Nijmegen.

4.4 Ontwerpbestemmingsplan Nijmegen Westkanaaldijk 2016 - 3 (Hogelandseweg 104)

Besluit

1. Het ontwerpbestemmingsplan Nijmegen Westkanaaldijk 2016 - 3 (Hogelandseweg 104) vrij te geven voor ter visie legging, overeenkomstig de geometrisch bepaalde planobjecten als vervat in het bestand NL.IMRO.0268.BPa10503-ON01 met bijbehorende bestanden;
2. Geen m.e.r.-procedure voor het bestemmingsplan te doorlopen.

Besluitenlijst Collegevergadering

Datum 16-04-2019
Tijd 9:00 - 12:30
Locatie SH - Trêveszaal

Aanwezigen

Voorzitter H. Bruls

Wethouders M. Esselbrugge, B. Frings, R. Helmer, Harriet Tiemens, Bert Velthuis, Noël Vergunst
en Grete Visser

Gemeentesecretaris Arne van Hout

Communicatie Freico Amberg

Notulist Mido Sofovic

Aldus vastgesteld in de vergadering van:
7 mei 2019

De voorzitter,

De secretaris,

1.0 Vastgesteld met machtiging tot aanpassing

1.1 Brief coalitieonderhandelingen Provincie

Besluit

1. Brief aan de coalitieonderhandelaars van de provincie Gelderland vast te stellen.

3.0 Vaststellen bespreekvoorstellen

3.1 Stadsrekening 2018

Besluit

Aan de Raad voor te stellen

1. De Stadsrekening 2018 vast te stellen.
2. Het nadelig jaarrekeningresultaat van € 897.735 te onttrekken aan de saldireserve.
3. Het voordelig resultaat van € 3.736.000 van het product beschermd wonen en vrouwenopvang, onderdeel van het programma Zorg & Welzijn te storten in de bestemde "regionale" reserve WMO beschermd wonen, door een onttrekking uit de saldireserve.
4. a. Een bestemmingsreserve Decembercirculaire in te stellen.
b. De in 2018 ontvangen middelen algemene uitkering van € 4.484.943 voor beleidsdoelen die eerst in 2019 uitgevoerd kunnen worden, in de reserve te storten.
5. Een bestemmingsreserve onderhoud Rivierenpark in te stellen.
6. Het budget voor grenscorrectie van € 150.000 over te hevelen naar 2019.
7. De begrotingswijziging over investeringskredieten vast te stellen (BW-1664).
8. Voor topplaagrenovaties aan sportvelden een afschrijvingstermijn van 10 jaar te hanteren.

3.2 Bestemmingsplan Nijmegen Dukenburg - 14 (Winkelcentrum Meijhorst)

Besluit

Aan de raad voor te stellen:

1. De beoordeling van de ingekomen zienswijze over het ontwerpbestemmingsplan Nijmegen Dukenburg - 14 (Winkelcentrum Meijhorst) vast te stellen;
2. Het bestemmingsplan Nijmegen Dukenburg - 14 (Winkelcentrum Meijhorst) gewijzigd vast te stellen, overeenkomstig de geometrisch bepaalde planobjecten als vervat in het bestand NL.IMRO.0268.BP4014-VG01 met bijbehorende bestanden;
3. Geen exploitatieplan vast te stellen als bedoeld in artikel 6.12 Wet ruimtelijke ordening.

3.3 Versterking regionale samenwerking

Besluit

1. Akkoord te gaan met het starten van het voorgestelde proces vanuit de 18 regiogemeenten om de regionale samenwerking in de regio Arnhem-Nijmegen te versterken, waarbij het maken van een lange termijn visie en het ontwerpen van een daarbij passende governance de kern vormen.
2. Arnhem en Nijmegen het voortouw te laten nemen in dit proces;
3. Een stuurgroep te vormen met de burgemeesters van Arnhem en Nijmegen en evenredig aangevuld met bestuurders vanuit iedere sub-regio, die dit proces gaat sturen.
4. De discussienotitie Regionale samenwerking: Samen steviger en sterker (april 2019) van de Kring Gemeentesecretarissen regio Arnhem-Nijmegen daarbij als leidraad te gebruiken.
5. Brief aan de raad over deze in te zetten ontwikkeling vast te stellen.

3.4 Stads- en Wijkmonitor 2019

Besluit

1. Stads- en Wijkmonitor 2019 vast te stellen.
2. Brief aan de raad over de Stads- en Wijkmonitor 2019 vast te stellen.

3.5 Stadscentrummonitor 2018-2019, Monitor Vestigingsklimaat 2019 en Horecaonderzoek Binnenstad 2018-2019

Besluit

1. Stadscentrummonitor 2018-2019 vast te stellen.
2. Monitor Vestigingsklimaat 2019 vast te stellen.
3. Horecaonderzoek Binnenstad 2018-2019 vast te stellen.
4. Brief aan de raad over de Stadscentrummonitor 2018-2019, Monitor Vestigingsklimaat 2018-2019 en Horecaonderzoek Binnenstad 2018-2019 vast te stellen.

3.6 Wet verplichte ggz

Besluit

De raadsinformatiebrief over de implementatie van de Wet verplichte ggz vaststellen.

3.7 Regionale samenwerking de Hulsen (vanaf 2021)

Besluit

1. In te stemmen met de uitgangspunten en scenario opgenomen in de notitie 'Doordecentralisatie 2021: de Hulsen'.
2. De brief over de Hulsen vast te stellen.

4.0 Vaststellen conformvoorstellen

4.1 Bestemmingsplan Nijmegen Dijkzone – Hof van Holland

Besluit

Aan de raad voor te stellen:

1. Het bestemmingsplan “Nijmegen Dijkzone – Hof van Holland” ongewijzigd vast te stellen, overeenkomstig de geometrisch bepaalde planobjecten als vervat in het bestand NL.IMRO.0268.BP26500.VG01 met bijbehorende bestanden;
2. Beeldkwaliteitsplan Dijkzone vast te stellen;
3. Geen exploitatieplan vast te stellen als bedoeld in artikel 6.12 Wet ruimtelijke ordening.

4.2 Bestemmingsplan Nijmegen Dijkzone – Woenderskamp met bijbehorende beeldkwaliteitsplan

Besluit

Aan de raad voor te stellen:

1. Het bestemmingsplan “Nijmegen Dijkzone – Woenderskamp” gewijzigd vast te stellen, overeenkomstig de geometrisch bepaalde planobjecten als vervat in het bestand NL.IMRO.0268.BP27500.VG01 met bijbehorende bestanden;
2. Geen exploitatieplan vast te stellen als bedoeld in artikel 6.12 Wet ruimtelijke ordening.

4.3 Bestemmingsplan Groot Oosterhout - 10 (Griftdijk 62, 2 woningen)

Besluit

Aan de raad voor te stellen:

1. Het bestemmingsplan Groot Oosterhout – 10 (Griftdijk 62, 2 woningen) gewijzigd vast te stellen, overeenkomstig de geometrisch bepaalde planobjecten als vervat in het bestand NL.IMRO.0258.BP29010.VG01 met bijbehorende bestanden;
2. Geen exploitatieplan vast te stellen als bedoeld in artikel 6.12 Wet ruimtelijke ordening.

4.4 Bestemmingsplan Groot Oosterhout - 10 (Griftdijk 62, kinderdagverblijf)

Besluit

Aan de raad voor te stellen:

1. Het bestemmingsplan Groot Oosterhout – 7 (Griftdijk 62, kinderdagverblijf) gewijzigd vast te stellen, overeenkomstig de geometrisch bepaalde planobjecten als vervat in het bestand NL.IMRO.0258.BP29007.VG01 met bijbehorende bestanden;
2. Geen exploitatieplan vast te stellen als bedoeld in artikel 6.12 Wet ruimtelijke ordening.

4.5 Veiligheidsbrief 2019

Besluit

De brief aan de raad met als onderwerp: Veiligheidsbrief 2019, vast te stellen.

4.6 Voortgangsbrief Aardgasvrij

Besluit

1. De voortgangsbrief Aardgasvrij aan de raad vast te stellen.

4.7

ENSIA 2018

Besluit

1. Te verklaren dat bij gemeente Nijmegen op 31 december 2018 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet.
2. De bevestigingen aan de auditor 2Control af te geven zoals beschreven in de brief getiteld: LOR ENSIA Nijmegen 2018.
3. De Verantwoordingsrapportage BAG 2018 vast te stellen.
4. De Verantwoordingsrapportage BGT 2018 vast te stellen.
5. De Letter of Representation ENSIA Nijmegen 2018 vast te stellen.
6. De Rapportage Informatiebeveiliging en Privacy 2018 voor kennisgeving aan te nemen.
7. De brief aan de raad over Afronding verantwoording ENSIA 2018 vast te stellen.

4.8

Beantwoording schriftelijke vragen fractie D66 inzake aanmaning inwoners en terugvorderen bijstandsgelden en de gemeenteraad over het incassobeleid

Besluit

1. De brief aan de fractie van D66 'Beantwoording schriftelijke vragen inzake aanmaning en terugvorderen bijstandsgelden' Nijmegen vast te stellen.
2. De brief 'Toezegging informeren incassobeleid' aan de raad vast te stellen.

4.9

Subsidieaanvragen t.b.v. Nijmegen Klinkt!

Besluit

1. Aan Stichting Vlegel een subsidie van € 16.150,- te verlenen voor de organisatie van het festival Valkhof Klassiek als onderdeel van het evenement Nijmegen Klinkt! op 1 en 2 juni 2019 en het bedrag ten laste te brengen van het programma Cultuur en Cultureel erfgoed, deelproductnummer 60588.S.4057;
2. Aan Stichting Nijmeegs Muziekfestival een subsidie van € 16.165,- te verlenen voor de organisatie van het Nijmeegs Muziekfestival als onderdeel van het evenement Nijmegen Klinkt! op 1 en 2 juni 2019 en het bedrag ten laste te brengen van het programma Cultuur en Cultureel erfgoed, deelproductnummer 60588.S.4057;
3. Aan de Nijmeegse Federatie van Muziekverenigingen een subsidie van € 2.825,- voor de organisatie van de Streetparade als onderdeel van het evenement Nijmegen Klinkt! op 1 en 2 juni 2019 en het bedrag ten laste te brengen van het programma Cultuur en Cultureel erfgoed, deelproductnummer 60588.S.4057.

4.10

Subsidieverstrekking Stichting Sterker sociaal werk

Besluit

1. Voor de jaren 2019, 2020 en 2021 een meerjarige subsidie te verstrekken in totaal € 100.000,-. Voor 2020 en 2021 onder voorbehoud van vaststelling van de begroting van dat jaar door de raad.
2. De subsidie te dekken uit de daarvoor beschikbare middelen binnen de begroting van het Raadsprogramma Welzijn, Wijkontwikkeling en Zorg, taakveld 6.71 Maatwerkdienstverlening 18+.

4.11 Anterieure overeenkomst Bachstraat 29 Nijmegen

Besluit

1. Een anterieure overeenkomst met Joep Burghouts Beheer B.V. aan te gaan voor de herontwikkeling van de locatie Bachstraat 29 te Nijmegen.
2. De financiële verantwoording plaats te laten vinden binnen de planexploitatie G147 Bachstraat.

4.12 Verkoop perceel grond t.b.v. horecalocatie in deelgebied Grote Boel

Besluit

1. Te gunnen en te verkopen aan belanghebbenden een perceel grond voor de realisatie van horeca in deelgebied Grote Boel, op de plek van de voormalige boerderij Groote Boel aan de Louis Paul Boonstraat, kadastraal bekend gemeente Nijmegen, sectie E, nummer 1208.
2. Het afdelingshoofd van het Ontwikkelingsbedrijf te machtigen de overeenkomst verder in detail uit te werken.
3. De financiële verantwoording plaats te laten vinden binnen de planexploitatie G283621 (verkoop Grote Boel).

Besluitenlijst Collegevergadering

Datum 10-07-2018
Tijd 9:00 - 12:30
Locatie SH - Trêveszaal
Voorzitter

Aanwezigen

Voorzitter H. Bruls
Wethouders M. Esselbrugge, B. Frings, R. Helmer, H. Tiemens, B. Velthuis, N. Vergunst en G. Visser
Gemeentesecretaris A. van Hout
Communicatie J. Broeksteeg
Notulist M. Sofovic

Aldus vastgesteld in de vergadering van:
28 augustus 2018

De voorzitter,

De secretaris,

3.0 Vaststellen bespreekvoorstellen

3.1 Monitoring prestatieafspraken met woningcorporaties en huurdersorganisaties 2017

Besluit

1. Kennis te nemen van de behaalde resultaten door de woningcorporaties over het jaar 2017.
2. De brief aan de raad over monitoring prestatieafspraken woningcorporaties en huurdersorganisaties vaststellen.

3.2 Koopoptie op verwerving opstalrecht op het Goffertstadion

Besluit

1. De koopoptie op verwerving van het opstalrecht op het Goffertstadion, opgenomen in bijlage 1, vast te stellen.
2. De brief aan de raad, waarin we een reactie geven op de wensen en bedenkingen en tevens aangeven dat de Europese Commissie geen aanleiding ziet om te constateren dat er sprake is van staatssteun, vast te stellen.

3.4 Bestuursovereenkomst PHS Nijmegen en westelijke stationsentree

Besluit

1. De Bestuursovereenkomst (BOK) PHS Nijmegen - westelijke stationsentree gemeente Nijmegen met het Ministerie van Infrastructuur en Waterstaat vast te stellen.

Ter besluitvorming door de burgemeester:

2. Wethouder H. Tiemens te mandateren de Bestuursovereenkomst PHS Nijmegen - westelijke stationsentree op 12 juli a.s. samen met de staatssecretaris S. van Veldhoven te ondertekenen.

3.6 Voortgangsrapportage Interventieplan Zorg en Welzijn (Fase 2) 2018 - Kwartaal 1

Besluit

1. De Voortgangsrapportage Interventieplan Zorg en Welzijn 2018 (fase 2) -Kwartaal 1 vast te stellen.
2. De brief aan de raad inzake de voortgangsrapportage Interventieplan Zorg en Welzijn 2018 (fase 2) – Kwartaal 1 vast te stellen.

3.7 Overzicht uitvoering aanvaarde raads moties tot en met 16 mei 2018

Besluit

Aan de raad voor te stellen

1. De voortgangsmeldingen vast te stellen.
2. De moties met de volgende volgnummers uit het voortgangsoverzicht af te voeren:
1, 8, 10, 11, 15, 22, 23, 25, 27, 28, 29, 30, 37, 39, 40, 44, 45, 54, 55, 56, 57, 59, 60, 61, 62, 66, 67, 71, 72.

3.8 Intentieovereenkomst locatieonderzoek Orbis - experience op gebied van duurzaamheid

Besluit

1. Intentieovereenkomst met Orbis Experience vast te stellen over een locatiestudie en haalbaarheidsonderzoek naar vestiging van deze innovatieve experience in Nijmegen.

3.9 Uitvoeringsplan Diversiteit en Inclusiviteit gemeente Nijmegen

Besluit

1. Het Uitvoeringsplan Diversiteit en Inclusiviteit voor de gemeente Nijmegen vast te stellen.
2. De brief aan de raad over het Uitvoeringsplan Diversiteit en Inclusiviteit voor de gemeente Nijmegen vast te stellen.

3.10 Variantenstudie ontsluiting woningbouw in park Waaijenstein

Besluit

1. De 14 kavels Waaijenstein en 7 landgoedwoningen (landgoed Oosterhout) te laten ontsluiten via de Volsellastraat en het appartementencomplex in Waaijenstein laten ontsluiten via een nieuwe ontsluiting naar Woenderskamp.
2. De uitwerking van de ontsluiting, mede in relatie tot de inrichting van park Waaijenstein in samenspraak met de omgeving tot stand laten komen.
3. Brief aan de raad over het besluit van de ontsluiting van de woningen in Waaijenstein en de financiële impact daarvan vast te stellen.

3.11 Besluit brandveilig gebruik en basishulpverlening overige plaatsen

Besluit

De raadsbrief inzake het Besluit brandveilig gebruik en basishulpverlening overige plaatsen vast te stellen.

3.12 Brief beantwoording vragen Technische Toelichting Zandafvoer Beuningen

Besluit

De brief over de beantwoording van vragen van de Technische Toelichting over de Zandafvoer Beuningen vast te stellen

3.13 Beantwoording schriftelijke vragen fractie PvdA over 'onderwijs moet lonen'

Besluit

De beantwoordingsbrief aan fractie PvdA over 'onderwijs moet lonen' vast te stellen.

3.14 Beantwoording twee schriftelijke vragen Stadspartij DNF over een houdverbod bij verwaarlozing van huisdieren

Besluit

1. Vast te stellen dat wij niet bereid zijn samen met de G32 op te trekken om bij het Rijk een houdverbod voor huisdieren af te dwingen voor baasjes die hun dieren mishandelen of verwaarlozen, omdat de gemeentelijke bevoegdheden zich niet tot de omgang met huisdieren uitstrekken.
2. De brief aan Stadspartij DNF over het instellen van een houdverbod bij verwaarlozing van huisdieren vast te stellen.

3.15 Koers Stadscontrol

Besluit

1. De inhoudelijke aandachtsgebieden van Stadscontrol vast te stellen, te weten: kaders stellen aan en faciliteren van gemeentebrede organisatieontwikkeling, aanjagen van continu leren en verbeteren, toetsen, adviseren en initiëren van (verbeter)voorstellen, coördineren en regisseren van de informatiebeveiliging en toezicht op goed openbaar bestuur.
2. Stadscontrol als een aparte eenheid rechtstreeks bij de gemeentesecretaris te positioneren.
3. De aanstelling van plaatsvervangend stadscontroller per 10 juli 2018 te beëindigen.

3.16 Programmering investeringen Openbare Ruimte 2018

Besluit

1. De investeringskredieten voor het jaar 2018 zoals opgenomen in de Stadsbegroting 2018, als volgt te programmeren:
 - a. K000067 Groot- en vervangingsonderhoud verbijzonderen naar I-nrs ad € 5,3 mln;
 - b. K000212 Rioolinvesteringen Waalsprong verbijzonderen naar I-nrs ad € 3,4 mln;
 - c. K000265 Maatschappelijke investeringen in de openbare ruimte ad € 4,8 mln;
 - d. K000279 Onderhoud woonstraatjes ad € 2,5 mln.
2. Begrotingswijziging BW-01626, waarmee de verbijzondering verwerkt kan worden in de begroting, vast te stellen.

3.17 Aankoop Tweede Walstraat 104 - 106

Besluit

1. Te besluiten tot aankoop van het pand de Tweede Walstraat 104 -106.

3.18 Zienswijze op Provinciale Omgevingsvisie

Besluit

De reactiebrief op de ontwerp- Omgevingsvisie van de provincie Gelderland (Gaaf Gelderland) vast te stellen en te versturen.

3.19 Status stukken warmtenet

Besluit

1. De brief aan de rekenkamer vast te stellen

4.0 Vaststellen conformvoorstellen

4.1 Nijmeegse Kaderverordening Subsidies (NKS) 2019

Besluit

Onder voorbehoud van vaststelling van de Nijmeegse Kaderverordening Subsidies 2019 door de Raad, het Uitvoeringsvoorschrift subsidies Directie Inwoners gemeente Nijmegen (2011) in te trekken per 1 oktober 2018.

Aan de Raad voor te stellen:

1. De bijgevoegde Nijmeegse Kaderverordening Subsidies 2019 (NKS 2019) vast te stellen.
2. De Nijmeegse Kaderverordening Subsidieverstreking (2011) in te trekken per 1 oktober 2018.

4.2 Informeren van de raad over de afronding verantwoording ENSIA 2017

Besluit

1. Brief aan de raad over de afronding van de verantwoording ENSIA 2017 vast te stellen

4.3 Beantwoording vragen ex art. 39 over vergunningverlening kamerverhuur door Stadspartij DNF

Besluit

1. De brief aan Stadspartij DNF over vergunningverlening kamerverhuur vast te stellen.

4.4 Gunningsadvies collectieve aanvullende ziektekostenverzekering voor minima

Besluit

Conform het gunningsadvies op grond van de uitkomsten van de Europese openbare aanbesteding Collectieve aanvullende ziektekostenverzekering voor minima met ingang van 1 januari 2019 voorlopig te gunnen aan VGZ (IZA Zorgverzekeraar) en CZ Intermediair.

2. Nadat de bezwaartermijn van 20 kalenderdagen is verstreken en geen gerechtelijke procedure aanhangig is gemaakt definitief te gunnen en een overeenkomst aan te gaan met VGZ (IZA Zorgverzekeraar) en CZ Intermediair.

4.5 Overeenkomst advocaatdiensten

Besluit

De raamovereenkomst met Hekkelman Advocaten N.V. inzake het leveren van advocaatdiensten, vast te stellen.

4.6 Stichting de Vierdaagsefeesten, samenwerkingsovereenkomst 2019 t/m 2022

Besluit

De bijgevoegde samenwerkingsovereenkomst tussen de stichting Vierdaagsefeesten en gemeente Nijmegen 2019 tot en met 2022 vast te stellen.

4.7 Volwasseneneducatie Rijk van Nijmegen 2018 e.v.

Besluit

1. In te stemmen met het ondertekenen van de Samenwerkingsovereenkomst Volwasseneneducatie en de bijdrage aan het regionaal contractmanagement te dekken uit het programma Onderwijs.
2. In te stemmen met het Regionaal Programma Laaggeletterdheid en Volwasseneneducatie en de investering in de regionale infrastructuur te dekken uit het programma Onderwijs.
3. In te stemmen met de aanstelling van de taalcoördinator.

Ter besluitvorming door de burgemeester

1. Wethouder Visser te machtigen de Samenwerkingsovereenkomst Volwasseneneducatie te ondertekenen.

4.8 Subsidievoorstel peuteropvang VVE 2018

Besluit

1. Kion een subsidie voor peuteropvang VVE te verlenen van € 1.004.065 voor de maanden augustus tot en met december 2018.
2. Kion een maatwerksubsidie te verlenen van € 64.215 voor de maanden augustus tot en met december 2018.
3. Kinop een subsidie voor peuteropvang VVE te verlenen van € 142.801 voor de maanden augustus tot en met december 2018.
4. Kinop een maatwerksubsidie te verlenen van € 38.776 voor de maanden augustus tot en met december 2018.
5. De subsidies voor Kinop en Kion van in totaal € 1.249.857 te dekken uit het deelproduct Peuterspeelzaalwerk (60634.S0941.44015).

4.9 Subsidieverlening vier hobbycentra 2018

Besluit

1. Een subsidie van in totaal € 714.749 te verlenen aan de vier hobbycentra in 2018.
2. De subsidie als volgt te verdelen: Hobbycentrum Nijmegen € 375.316, Hobbycentrum Nijmegen West € 93.764, Creatief Centrum Nijmegen Zuid € 95.004, Hobbycentrum Nijmegen Oost € 150. 665.
3. Een bedrag van € 714.751 ten laste te brengen van het programma Zorg & Welzijn, product Inclusieve wijknetwerken (61304 S3229 en S3610).

4.10 Subsidieregeling Amateurkunst Nijmegen

Besluit

1. De Subsidieregeling Amateurkunst Nijmegen 2017 per 1 januari 2019 in te trekken;
2. De Subsidieregeling Amateurkunst Nijmegen 2019 vast te stellen.

4.11 Verkoop woning Nederheidseweg 132, Nijmegen

Besluit

Te verkopen aan de heer F.H. Meulenveld en mevrouw A.Y. Roering de woning met omliggende grond Nederheidseweg 132, Nijmegen, groot ca 4855 m2, onder de voorwaarden en bepalingen zoals vermeld in bijgaande koopovereenkomst.

Besluitenlijst Collegevergadering

Datum 12-05-2020
Tijd 9:00 - 10:30
Locatie Vergadercentrum stadhuis

Aanwezigen

Voorzitter H. Bruls
Wethouders M. Esselbrugge, R. Helmer, H. Tiemens, B. Velthuis, N. Vergunst en G. Visser
Gemeentesecretaris A. van Hout
Communicatie J. Broeksteeg
Notulist M. Sofovic

Aldus vastgesteld in de vergadering van:
19 mei 2020

De voorzitter

De secretaris

2.0 Vaststellen aangehouden voorstellen

2.1 Zienswijze Jaarrekening 2019 en Ontwerpbegroting 2021 MGR Rijk van Nijmegen

Besluit

Aan de raad voor te stellen:

1. De zienswijze op de jaarrekening 2019 en de ontwerpbegroting 2021 van de MGR zoals verwoord in dit voorstel vast te stellen.
2. De brief aan het Dagelijks Bestuur van de MGR met de zienswijze op de jaarrekening 2019 en de ontwerpbegroting 2021 van de MGR vast te stellen.

2.2 Aanpassing bestuurlijke inrichting MGR

Besluit

Aan de raad voor te stellen:

1. De wijzigingen in de MGR conform het bijgaande wijzigingsbesluit vast te stellen.

3.0 Vaststellen bespreekvoorstellen

3.1 Antwoorden raadsvragen Stadsrekening 2019

Besluit

De brief aan de Raad met antwoorden op raadsvragen over de Stadsrekening 2019 vast te stellen.

3.2

Tweede maatregelenpakket Corona

Besluit

Het nemen van de volgende maatregelen om de effecten van de coronacrisis te verzachten:

1. Verlengen van het maatregelenpakket, zoals dat is vastgesteld d.d. 24 maart jl., voor de periode tot 1 juli 2020.
2. Het bovengenoemde maatregelenpakket op onderdelen aan te vullen of aan te scherpen, te weten:
 - Met maatwerk in stand houden van instellingen die de cruciale culturele infrastructuur vormen;
 - Opschorten van de huur tot 31 december 2020;
 - Actief invorderen van opgelegde parkeerbelasting (boetes).
 - Actief invorderen overige zaken (o.a. ozb en incasso)
3. Nieuwe maatregelen vast te stellen om ook ten tijde van de coronacrisis de sociale doelstellingen voor de stad te kunnen realiseren. Het gaat om de volgende maatregelen:
 - Compensatie voor de bijdrage van ouders die niet aanmerking komen voor kinderopvangtoeslag gedurende de sluiting van de kinderopvang;
 - Inrichten van een digitaal platform voor de uitwisseling van personeel.
4. Nieuwe maatregelen vast te stellen om ondanks de coronacrisis een basisniveau van culturele voorzieningen en evenementen in de stad te behouden en de sociale verbinding te versterken. Het gaat om de volgende maatregelen:
 - Financiële ondersteuning voor de meest vitale en beeldbepalende Nijmeegse evenementen;
 - Coullance met subsidies aan evenementen, waaronder de st. DE4DAAGSE en de st. Vierdaagsefeesten;
 - Kwijtschelden reclameopbrengsten evenementen
 - Stimuleren van tijdelijke alternatieven en evenementen binnen de op dat moment geldende richtlijnen;
 - Onderzoeken mogelijkheden steunfonds voor de 1,5 meter samenleving;
 - Subsidieregeling voor Corona Cultuurprojecten 2020;
 - Sensoren in de binnenstad benutten om passantenstromen te spreiden.
 - Inrichten van een Anderhalve Meter Loket en verruimde mogelijkheden voor terrassen.
 - Ketensolidariteit in de vastgoedsector stimuleren.
5. Nieuwe maatregelen vast te stellen om de werkgelegenheid en bedrijvigheid in de stad te behouden en de financiële effecten voor ondernemers te verzachten. Het gaat om de volgende maatregelen:
 - Ondersteuning horeca: geen precario voor terrassen in 2020;
 - Geen marktgelden innen in het 2^e en 3^e kwartaal van 2020;
 - Geen precario voor standplaatsen in het 2^e en 3^e kwartaal 2020;
 - Geen huur en leges voor evenementen in de periode 1 september t/m 31 december;
 - Actief bijdragen aan toerisme: promotie- en marketingcampagne voor de stad.
6. Nieuwe maatregelen vast te stellen, zodat we ondanks de coronacrisis kunnen blijven werken aan onze ambities op het gebied van duurzaamheid. Het gaat om de volgende maatregel:
 - Plan opstellen om Nijmegen duurzaam door de coronacrisis te loodsen;

- Bedrijven met “powernaps” blijven uitdagen om werk te maken van energietransitie.
- 7. Nieuwe maatregel vast te stellen om als moderne overheid wendbaar te zijn en ons aan te passen de nieuwe manier van werken binnen de anderhalve meter-samenleving: -
 - Onderzoek naar de impact van corona op de interne organisatie.
- 8. De financiële effecten van de te nemen maatregelen op de aangegeven wijze te verwerken.
- 9. De bijgevoegde brief aan de raad vast te stellen.

3.3 COVID-19: van noodmaatregelen naar afschaling, nazorg en herstel

Besluit

1. In te stemmen met het voorstel van het Regionaal Beleidsteam (RBT) van de Veiligheidsregio Gelderland-Zuid om ten behoeve van de transitie van de COVID-19 crisisbeheersing naar nazorg en herstel naast de crisisorganisatie een regionaal transitieteam in het leven te roepen die tot doel heeft om de gemeenten te adviseren in het proces van afschaling. De uitgangspunten hiervoor zijn geformuleerd in de notitie, d.d. 21 april 2020, getiteld: Naar een nieuwe fase in de crisis in Gelderland-Zuid – van noodmaatregelen naar afschaling, nazorg en herstel.

3.4 Subsidieregeling Corona Cultuurprojecten 2020

Besluit

1. De Subsidieregeling Corona Cultuurprojecten 2020 vast te stellen.

3.5 Erfgoedstrategie 2020

Besluit

1. De opgaven uit de erfgoedstrategie als uitgangspunt te nemen bij het erfgoedbeleid en bij de uitwerking van de Erfgoedstrategie prioriteit te geven aan:
 - a. Versterking wettelijke taken
 - b. Instellen erfgoedbeheerder voor 3 jaar
 - c. Publieksbereik en beleving Limes / Romeins erfgoed
2. De keuzes voor de investeringen na bespreking van de Erfgoedstrategie in de raad mee nemen bij de integrale afwegingen van de begroting.

Aan de raad voor te stellen:

1. De drie opgaven van de Erfgoedstrategie op hoofdlijnen vast te stellen:
 - a. betere instandhouding en bescherming
 - b. krachtiger publieksbereik door professionalisering, regie en samenwerking
 - c. inzet op profilering als oudste stad

3.6 Monitoring Groenestraat

Besluit

1. De brief over de resultaten van de monitoring aan de raad vast te stellen.

3.7 Annuleren compliment inclusieve sportvereniging 2020

Besluit

1. De uitreiking van het compliment inclusieve sportvereniging in 2020 te annuleren;
2. De brief aan de raad over het annuleren van het compliment inclusieve sportvereniging in 2020 vast te stellen.

3.8 Zienswijze Jaarstukken 2019, Begroting 2021 en Meerjarenraming 2022-2024 Omgevingsdienst Regio Nijmegen (ODRN)

Besluit

Aan de raad voor te stellen:

1. De adviezen van de Adviesfunctie Gemeenschappelijke Regelingen over de Jaarrekening 2019 en de Begroting 2021 over te nemen:
In te stemmen met de Jaarrekening 2019 van de gemeenschappelijke regeling Omgevingsdienst Regio Nijmegen.
In te stemmen met de voorgestelde resultaatbestemming, zijnde: het voordelig rekeningresultaat ad € 20.617,--, toe te voegen aan de algemene reserve.
In te stemmen met de Begroting 2021 (inclusief de extra tariefsverhoging van € 6,-- en inclusief de Ontwikkelagenda) met uitzondering van de niet toegepaste generieke korting van 1%.
Kennis te nemen van de Meerjarenraming 2022-2024.
2. De brief aan het Algemeen Bestuur van de ODRN over de zienswijze op de Jaarstukken 2019, Begroting 2021 en Meerjarenraming 2022-2024 vast te stellen, waarin tevens de aanvullende adviezen van de AGR zijn opgenomen.

4.0 Vaststellen conformvoorstellen

4.1 Zienswijze Wet voorkeursrecht gemeenten Winkelsteeg

Besluit

Aan de raad voor te stellen:

1. Het agendapunt 8 'Wet voorkeursrecht gemeenten Winkelsteeg' (35/2020) op de agenda van de Raad van de besluitronde van 10 juni 2020 af te voeren van de agenda en te besluiten op basis van dit raadsvoorstel dat daarvoor in de plaats treedt.
2. Op grond van artikelen 2 en 5 Wet voorkeursrecht gemeenten (Wvg) over te gaan tot aanwijzing van percelen en perceelgedeelten waarop de artikelen 10 tot en met 15, 24 en 26 Wvg van toepassing zijn. Het betreft de percelen en perceelgedeelten zoals aangegeven op de bij dit besluit behorende kadastrale tekeningen met nummers 558937 en 558938 en de bij dit besluit behorende percelenlijst.
3. Dat de toegedachte bestemming voor het gebied intensieve bedrijvigheid en wonen is en daarmee afwijkt van het huidig gebruik.
4. Dat er zal worden overgegaan tot het vaststellen van een structuurvisie ten behoeve van deze beoogde ontwikkeling.
5. De zienswijze niet over te nemen en de zienswijzennota vast te stellen.

4.2 **Zienswijze jaarstukken Gemeenschappelijke Regeling (GR) Bijsterhuizen**

Besluit

1. Zienswijze vast te stellen, waarbij we instemmen met de voorliggende jaarrekening 2019, begroting 2020 en meerjarenbegroting 2021-2024 en het voornemen tot winstneming van de GR Bijsterhuizen.
2. De brief aan het bestuur van de GR Bijsterhuizen vast te stellen.

4.3 **Zienswijze op jaarrekening 2019 en begroting 2021 Veiligheidsregio Gelderland-Zuid (VRGZ)**

Besluit

Aan de raad voor te stellen:

1. In te stemmen met de jaarrekening 2019 van de VRGZ en het resultaatbestemmingsvoorstel.
2. In te stemmen met de begroting 2021 van de VRGZ.
3. De meerjarenraming 2022-2024 voor kennisgeving aan te nemen.
4. De zienswijzebrief vast te stellen.

4.4 **Zienswijze conceptbegroting 2021, Begrotingswijziging Veilig Thuis 2020 en jaarrekening 2019 GGD Gelderland Zuid**

Besluit

1. De budgetsubsidies Nijmegen aan de GGD Gelderland Zuid voor het jaar 2019 (conform tabel 1) voor een bedrag van € 1.028.397 definitief vast te stellen.
2. Onder voorbehoud van vaststelling van de zienswijze over de begrotingswijziging 2020 en begroting 2021 van de GGD, de uitzetting van de kosten voor indexering, huisvesting, het Rijksvaccinatieprogramma en Veilig Thuis en de forensische dienstverlening te dekken uit de programmabegroting Welzijn, Wijkontwikkeling en Zorg.

Aan de raad voor te stellen:

1. Onze zienswijze over voorliggende concept jaarrekening 2019, de begrotingswijziging Veilig Thuis 2020 en de conceptbegroting 2021 van de GGD Gelderland Zuid vast te stellen.

Conform de zienswijze stemmen wij voor de jaarrekening 2019 in met:

- Vaststelling van de jaarrekening 2019, inclusief subsidies, met uitzondering van de subsidies genoemd in tabel 1, kolom C (bijlage bij de brief aan de GGD);
- Toevoegen van het positief resultaat van € 41.000 aan de algemene reserve van de GGD;
- Het vormen van een bestemde reserve van € 504.000 frictiekosten huisvesting.

Conform de zienswijze stemmen wij voor de begrotingswijziging Veilig Thuis 2020 in met:

- De keuze voor scenario 1 met daarin opgenomen groeipercentages voor “Adviezen en Meldingen” van respectievelijk 20% en 10% én de opgenomen verhouding tussen “Onderzoek en Voorwaarden & Vervolg” van 30% - 70%;
- De inzet van 12 uur monitoring i.p.v. 15 uur met ingang van 2020;
- Een structureel hogere bijdrage van € 445.115 (aandeel Nijmegen € 141.936);
- De inzet van incidentele middelen voor inwerktijd medewerkers van € 201.216;
- De inzet van incidentele middelen voor het zicht houden op veiligheid van € 200.000.

Conform de zienswijze stemmen wij voor de begroting 2021 in met:

- De keuze bij VT voor scenario 1 met daarin de opgenomen verhouding tussen “Onderzoek en Voorwaarden & Vervolg” van 30% - 70%;
- De inzet van 12 uur voor de monitoringfunctie bij VT in 2021, waarmee een deel van de opgelegde taakstelling voor 2021(1%), 2022 (2%) en 2023 (3%) ev. wordt ingevuld;
- De overheveling van het Zicht op Veiligheid uit het uniforme takenpakket naar een facultatieve taak per gemeente;
- De doorwerking van het structurele deel van de begrotingswijziging 2020 Veilig Thuis naar 2021 e.v.
- De wijze waarop de GGD invulling heeft gegeven aan de bezuinigingstaakstelling van 1% op de begroting 2021 voor een bedrag van € 453.000;
- Een structurele extra bijdrage voor de stijging van de lasten voor nieuwbouw GGD van € 95.475 (aandeel Nijmegen € 30.237 voor 2021);
- Een indexering van de uniforme inwonersbijdrage voor 2020 met 4,56% (zijnde € 1.059.743, aandeel Nijmegen € 418.396);
- Een uitzetting van de lasten voor 2021 met € 79.272 (aandeel Nijmegen € 20.845) voor het Rijksvaccinatieprogramma;
- Een a-structurele uitzetting van de lasten voor Forensische Dienstverlening van € 25.000 (aandeel Nijmegen € 7.918);
- Een correctie op inwoneraantallen binnen de regio Gelderland Zuid op grond waarvan de uniforme bijdragen per gemeente worden bepaald.

Wij stemmen niet in met:

- Het in scenario 1 opgenomen groeipercentage van 10% voor “Adviezen en Meldingen” en daarmee gepaard gaande uitzetting van € 674.000 (aandeel Nijmegen € 273.000).

Verder:

- Wensen wij een toelichting :
 - o op de gebruikte normtijden zoals toegepast in de begroting(swijziging) voor Veilig Thuis;
 - o op de verdubbeling van het aantal casussen “Huisverbod” bij Veilig Thuis;
 - o op het waarom Veilig Thuis ook voor 2021 een groei van 10% verwacht op het aantal “Adviezen en Meldingen”.
- Willen wij met de GGD in gesprek over de voorwaarden van facultatieve inzet van het product Zicht op Veiligheid, Psychosociale Hulp bij Incidenten en Overbruggingszorg voor JGZ.
- De brief aan de GGD Gelderland Zuid betreffende onze zienswijze over voorliggende conceptbegroting 2021 en concept jaarrekening 2019 vast te stellen.

- De incidentele kosten voor Veilig Thuis voor 2020 van € 401.216 éénmalig te dekken uit de Bestemmingsreserve beschermd wonen/vrouwenopvang middels bijgevoegde begrotingswijziging.
- Bijgevoegde begrotingswijziging BW-01737 vast te stellen.

4.5 Zienswijze Begroting 2021-2024 Bedrijfsvoering organisatie Doelgroepenvervoer Regio Arnhem-Nijmegen (BVO DRAN)

Besluit

Aan de raad voor te stellen:

1. Kennis te nemen van de ontwerp- meerjarenprogrammabegroting 2021-2024 (inclusief gewijzigde begroting 2020) van Bedrijfsvoeringsorganisatie Doelgroepenvervoer regio Arnhem Nijmegen (BVO DRAN), zoals die op 2 april 2020 door het algemeen bestuur is vastgesteld.
2. De brief met de zienswijze op de ontwerp-begroting 2021-2024 (inclusief gewijzigde begroting 2020) vast te stellen en deze vóór 15 juni 2020 aan het bestuur van BVO DRAN te verzenden.

4.6 ENSIA 2019

Besluit

- Te verklaren dat bij gemeente Nijmegen op 31 december 2019 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet.
- De bevestigingen aan de auditor 2Control af te geven zoals beschreven in de brief getiteld: LOR ENSIA Nijmegen 2019.
- De verantwoordingsrapportage BAG 2019 vast te stellen.
- De verantwoordingsrapportage BGT 2019 vast te stellen.
- De verantwoordingsrapportage BRO 2019 vast te stellen.
- De Letter of Representation ENSIA Nijmegen 2019 vast te stellen.
- De brief terugkoppeling ENSIA BAG 2018 zelfevaluatie voor kennisgeving aan te nemen.
- De rapportage Informatiebeveiliging en Privacy 2019 voor kennisgeving aan te nemen.
- De brief aan de raad over ENSIA 2019 vast te stellen..
- Met toepassing van artikel 55, eerste lid van de Gemeentewet, in verband met artikel 10, tweede lid onder b en g van de Wet openbaarheid van bestuur, onszelf geheimhouding op te leggen op de als geheim aangeduide, gehele rapportage Informatiebeveiliging en Privacy 2019, verstrekt als bijlage bij de brief aan de gemeenteraad.
- Met toepassing van artikel 25, tweede lid van de Gemeentewet, in verband met artikel 10, tweede lid, onder b en g van de Wet openbaarheid van bestuur, aan de raad geheimhouding op te leggen de gehele rapportage Informatiebeveiliging en Privacy 2019, verstrekt als bijlage bij de brief aan de gemeenteraad.

Aan de raad voor te stellen:

op grond van artikel 25 derde lid van de Gemeentewet, in de eerst volgende vergadering van de Raad de door het College van B&W van 12 mei 2020 opgelegde geheimhouding te bekrachtigen.

4.7 Ontwikkelingen Spoorkuil, Bottendaalzijde

Besluit

1. In te stemmen met de koopovereenkomst Dr Jan Berendsenstraat 47-67 en de opbrengst aan te wenden voor het verwerven van de gronden van NS Vastgoed, onder voorwaarde van instemming van de Raad met de planexploitatie Spoorkuil.
2. In te stemmen met de eeuwigdurende erfpachtovereenkomst Spoorkuil Bottendaalzijde met NS Vastgoed, onder voorwaarde van instemming van de Raad met de planexploitatie Spoorkuil.
3. In te stemmen met het in beheer brengen van de gronden aan de Spoorkuil aan de werkgroep Bottendaal en daar nadere afspraken over te maken met de afdeling stadsbeheer.
4. Te verkennen wat de ontwikkelingsmogelijkheden zijn van het Seinhuisje.

Aan de raad voor te stellen:

1. Voor het structureel behouden en in groengebruik geven van de gronden in de Spoorkuil Bottendaalzijde aan de bewoners van Bottendaal de bijbehorende planexploitatie Spoorkuil vast te stellen.
2. De financiële gevolgen – voor zover niet betrekking hebbende op de planexploitatie – bij de zomernota 2020 te verwerken.

4.8 Evaluatie commissie Beeldkwaliteit

Besluit

1. Het evaluatierapport over de commissie Beeldkwaliteit 'Samen werken aan omgevingskwaliteit' vast te stellen.
2. Kennis te nemen van het Beeldend jaarverslag 2017-2019.
3. De brief aan de raad over het evaluatierapport 'Samen werken aan de omgevingskwaliteit' vast te stellen.

4.9 Beantwoording schriftelijke vragen van de Partij voor de Dieren en de SP over huwelijksvoltrekkingen tijdens de coronacrisis en het ontslag van een trouwambtenaar

Besluit

1. De brief aan de fractie van de Partij voor de Dieren, met beantwoording van de vragen over huwelijksvoltrekkingen en babsen tijdens de coronacrisis, vast te stellen.
2. De brief aan de fractie van de SP, met beantwoording van de vragen over het ontslag van een trouwambtenaar, vast te stellen.

4.10 Beantwoording schriftelijke vragen van de raadsfractie van Stadspartij DNF over overlast Waalkade/Lage Markt

Besluit

De brief aan de raadsfractie van Stadspartij DNF met als onderwerp: overlast Waalkade/Lage Markt, vast te stellen.

4.11 Brief bewoners flat Palazzo Lent

Besluit

1. De antwoordbrief aan de bewoners van flat Palazzo in Lent, die bezwaren hebben tegen de aanleg van een Tiny Forest door IVN Natuureducatie, vast te stellen.

4.12 Adviescommissie Beeldende Kunst, bemensing en reglement

Besluit

1. Een nieuw lid voor de commissie beeldende kunst, mevrouw C. Linders, te benoemen voor een termijn van 4 jaar.
2. Het lidmaatschap voor de commissie beeldende kunst voor de heer A. ter Avest te verlengen met 3 jaar.
3. Het voorzitterschap van de heer J.H. Daniels te verlengen voor maximaal 4 jaar.
4. De verordening commissie beeldende kunst, op 7 oktober 2003 door ons college vastgesteld, in te trekken en bijgaand reglement van de commissie beeldende kunst vast te stellen.
5. Brieven aan de betrokkenen vast te stellen.

4.13 Nieuwe ronde Individuele Plaatsing en Steun-trajecten Rijk van Nijmegen

Besluit

1. Aan WerkBedrijf Rijk van Nijmegen uit de ambulantiseringmiddelen GGZ voor Centrumgemeente Nijmegen van 2020 t/m 2023 een meerjarige subsidie - voor de periode 2020 t/m 2023 - van € 500.000 te verlenen voor de uitvoering van 62 IPS-trajecten voor kandidaten uit het Rijk van Nijmegen, onder voorbehoud van de vaststelling van de stadsbegroting over betreffende jaren.
2. De Subsidieregeling Individuele Plaatsing en Steun Rijk van Nijmegen 2020 vast te stellen en daarmee WerkBedrijf Rijk van Nijmegen te mandateren om subsidie te verlenen voor de uitvoering van IPS-trajecten (artikel 3) en hiervoor beleidsregels en nadere regels vast te stellen (artikel 4).

4.14 Regeling doorbraakbudget sociaal domein

Besluit

1. De regeling doorbraakbudget sociaal domein vast te stellen;
2. De procesregisseurs, de doorbraakcoaches en het overleg passende hulp te mandateren voor de uitvoering van de regeling.

4.15 Invullingsvoorstel krediet toegankelijkheid

Besluit

1. Het beschikbare krediet van K00268 in te zetten voor aanpassingen om de toegankelijkheid te vergroten op de volgende locaties:
 - a. Cortenaerpad 1 (sportzaal Bottendaal);
 - b. Smidstraat 31 (sportzaal Onder de St. Steven);
 - c. Zwaluwstraat 200 (sportzaal Zwaluw);
 - d. Korte Nieuwstraat 6 (Stadhuis);
 - e. Tolhuis 4450 (Open Wijkschool);
 - f. Archimedesstraat 9 (wijkcentrum De Schakel);
 - g. Daniëlsplein 3 (wijkcentrum Heseweide);
2. Begrotingswijziging BW-01732 vast te stellen.
3. De portefeuillehouder te machtigen de definitieve invulling van de posten vast te stellen.

Aan de gemeenteraad van Nijmegen

Postadres

Gemeente Nijmegen
FA20
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

Datum 16 april 2019

Betreft Afronding verantwoording ENSIA 2018

Geachte leden van de raad,

Conform afspraken met de VNG verantwoordt de gemeente Nijmegen zich met ingang van 2017 over Informatieveiligheid aan de raad door middel van een collegeverklaring ENSIA (Eenduidige Normatiek Single Information Audit). In deze brief informeren wij u over de ENSIA auditresultaten van 2018.

Het verantwoordingsstelsel ENSIA

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel om verantwoording over informatieveiligheid af te leggen aan de raad en het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren. Dit door het toezicht op informatiebeveiliging te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het college een verbeterd overzicht en sturingsmogelijkheden over informatiebeveiliging. Daarnaast structureert ENSIA tevens de verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Doordat alle verschillende verantwoordingsstelsels op elkaar aangesloten moeten worden, gold 2017 als overbruggingsjaar. 2018 is het eerste jaar waarin de ENSIA systematiek volledig werd toegepast over alle stelsels.

ENSIA audit 2018

De verantwoording is gebaseerd op een zelfevaluatie welke bestaat uit vragen die gebaseerd zijn op een aantal beheersmaatregelen op het vlak van informatieveiligheid. Deze zelfevaluatie is beoordeeld door een onafhankelijke auditor.

De Collegeverklaring

Het resultaat van de ENSIA audit wordt verwoord in de Collegeverklaring ENSIA 2018 (vastgesteld op 16 april 2019) waarin verklaard wordt dat bij gemeente Nijmegen op 31 december 2018 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de

geselecteerde normen inzake DigiD en Suwinet. Voor het afleggen van verantwoording aan de gemeenteraad wordt er aangesloten bij de planning en control cyclus. In het jaarverslag is daarom een passage opgenomen over de stand van zaken met betrekking tot informatieveiligheid. Meer onderbouwing en verdieping op dit onderwerp is te vinden in de Rapportage Informatiebeveiliging en Privacy 2018 die bij deze brief wordt aangeboden.

Hoogachtend,
Het college van burgemeester en wethouders van Nijmegen

mr. drs. A.H. van Hout
gemeentesecretaris

drs. H.M.F. Bruls
burgemeester

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

E20.001168

Datum 12 mei 2020

Betreft Afronding verantwoording ENSIA 2019

Geachte leden van de raad,

Conform afspraken met de VNG verantwoordt de gemeente Nijmegen zich met ingang van 2017 over Informatieveiligheid aan de raad door middel van een collegeverklaring ENSIA (Eenduidige Normatiek Single Information Audit). In deze brief informeren wij u over de ENSIA auditresultaten van 2019.

Het verantwoordingsstelsel ENSIA

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel om verantwoording over informatieveiligheid af te leggen aan de raad en het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren. Dit door het toezicht op informatiebeveiliging te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het college een verbeterd overzicht en sturingsmogelijkheden over informatiebeveiliging. Daarnaast structureert ENSIA tevens de verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet). Het jaar 2019 is het tweede jaar waarin de ENSIA systematiek volledig werd toegepast over alle stelsels.

ENSIA audit 2019

De verantwoording is gebaseerd op een zelfevaluatie welke bestaat uit vragen die gebaseerd zijn op een aantal beheersmaatregelen op het vlak van informatieveiligheid. Deze zelfevaluatie is beoordeeld door een onafhankelijke auditor.

ENSIA resultaat

Het resultaat van de ENSIA audit wordt verwoord in de Collegeverklaring ENSIA 2019 (vastgesteld op 12 mei 2020). In deze Collegeverklaring wordt verklaard dat bij gemeente Nijmegen op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Voor het afleggen van verantwoording aan de gemeenteraad wordt er aangesloten bij de planning en control cyclus. In het jaarverslag is daarom een passage opgenomen over de stand van zaken met betrekking tot informatieveiligheid. Meer onderbouwing en verdieping op dit onderwerp is te vinden in de bijgesloten Rapportage Informatiebeveiliging en Privacy 2019. Hierin leest u dat er stappen gezet zijn op het vlak van met name infrastructuur en eigenaarschap. In deze context heeft met name Corsa prioriteit. Voor het komende jaar hebben iBewustzijn en monitoring van de informatie omgeving een belangrijk deel van de aandacht. Dit zodat wij blijven voldoen aan de normen voor DigiD en Suwinet, en daarnaast ook voortgang boeken op het voldoen aan andere kaders zoals de AVG (Algemene Verordening Gegevensbescherming).

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

mr. drs. A.H. van Hout
gemeentesecretaris

drs. H.M.F. Bruls
burgemeester

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

E21.000661

Datum 13 april 2021
Betreft Afronding verantwoording ENSIA 2020

Geachte leden van de raad,

Conform afspraken met de VNG verantwoordt de gemeente Nijmegen zich met ingang van 2017 over Informatieveiligheid aan de raad door middel van een collegeverklaring ENSIA (Eenduidige Normatiek Single Information Audit). In deze brief informeren wij u over de ENSIA auditresultaten van 2020.

Het verantwoordingsstelsel ENSIA

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel om verantwoording over informatieveiligheid af te leggen aan de raad en het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren. Dit door het toezicht op informatiebeveiliging te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het college een verbeterd overzicht en sturingsmogelijkheden over informatiebeveiliging. Daarnaast structureert ENSIA tevens de verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet). Het jaar 2020 is het derde jaar waarin de ENSIA systematiek volledig werd toegepast over alle stelsels.

ENSIA audit 2020

De verantwoording is gebaseerd op een zelfevaluatie welke bestaat uit vragen die gebaseerd zijn op een aantal beheersmaatregelen op het vlak van informatieveiligheid. Deze zelfevaluatie is beoordeeld door een onafhankelijke auditor.

ENSIA resultaat

Het resultaat van de ENSIA audit wordt verwoord in de Collegeverklaring ENSIA 2020 (vastgesteld op 13 april 2021). In deze Collegeverklaring wordt verklaard dat bij gemeente Nijmegen op 31 december 2020 voor DigiD en Suwinet nagenoeg aan de

normen wordt voldaan. Geconstateerd is dat de interne beheersingsmaatregelen, in opzet en bestaan, voor circa 95% voldoen aan de door de Rijksoverheid verplicht gestelde geselecteerde normen inzake de DigiD en Suwinet toepassingen die bij ons bekend waren. Wij hebben verbeterplannen opgesteld om zo snel mogelijk aan alle normen te voldoen. De acties zijn belegd en worden gemonitord.

Voor het afleggen van verantwoording aan de gemeenteraad wordt er aangesloten bij de planning en control cyclus. In het jaarverslag is daarom een passage opgenomen over de stand van zaken met betrekking tot informatieveiligheid. Meer onderbouwing en verdieping op dit onderwerp is te vinden in de bijgesloten Rapportage Informatiebeveiliging en Privacy 2020. Dit is een jaarlijks verslag waarin u leest over de partijen waar wij mee samenwerken, welke resultaten er bereikt zijn in 2020 en wat de verwachte ontwikkelingen zijn in de komende jaren. Dit zodat wij in 2021 voldoen aan de normen voor DigiD en Suwinet, en daarnaast ook voortgang boeken op het verbeteren van de informatieveiligheid en het voldoen aan andere kaders zoals de AVG (Algemene Verordening Gegevensbescherming).

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

mr. drs. A.H. van Hout
gemeentesecretaris

drs. H.M.F. Bruls
burgemeester

Bijlage: Rapportage IB en Privacy gemeente Nijmegen 2020 v 1

Rapportage Informatiebeveiliging en Privacy

Periode 2017



Inhoud

Rapportage	1
Informatiebeveiliging en Privacy	1
Periode 2017	1
Versiebeheer	3
Verspreiding	3
Doel en scope	4
Beleid en verantwoording	4
Informatiebeveiliging	4
Privacy	5
Algemeen Beeld en Resultaten	5
Beheersmaatregelen Informatiebeveiliging	7
Maatregelen belegd bij de iRvN	8
Samenwerkingen	9
Realisatie Doelstellingen	10
Meerjaren Perspectief	10
Informatiebeveiliging	10
Privacy	11

Versiebeheer

Versie	Datum	Opstellers	Opmerkingen
0.1	09-02-2018	Zijle0	Eerste concept
0.2	05-03-2018	Zijle0	Vervolg aanvullingen
0.3	12-03-2018	Zijle0	Opmerkingen Danny
0.4	13-03-2018	Zijle0, Jagen0	iRvN invoegen
0.5	23-03-2018	Zijle0	Input sijmr0
0.6	26-03-2018	Zijle0	Input jagen0
1.0	05-04-2018	Zijle0	Na PO

Verspreiding

De rapportage wordt opgesteld door de CISO, vastgesteld door het college en ter kennisname verstuurd aan directie en aan B&W. Het verslag bij de jaarrekening bevat in de paragraaf over bedrijfsvoering een passage over informatiebeveiliging en privacy. Dit document wordt via de website <http://pcportal.nijmegen.nl/> gepubliceerd. De rapportage die voor u ligt is een verdieping en verbreding op de passage in het jaarverslag.

Doel en scope

Gemeenten hebben in de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' van november 2013 onder meer afgesproken dat in het jaarverslag een aparte paragraaf over informatiebeveiliging wordt opgenomen. Dit is een van de maatregelen van het normenkader Baseline Informatiebeveiliging Gemeenten (BIG). Met deze paragraaf verantwoordt het college van B&W zich aan de gemeenteraad over informatiebeveiliging in brede zin. De separate jaarrapportage die hier voor ligt bevat de ontwikkelingen, activiteiten, incidenten en risico's met betrekking tot de onderwerpen informatieveiligheid en privacy bij de gemeente Nijmegen over het jaar 2017. Het geeft de ruimte om een beeld te schetsen van de ontwikkeldoelen voor de komende periode en de bedreigingen die van invloed zijn of kunnen zijn op de gemeente. De rapportage is in overeenstemming met het door het college vastgestelde informatiebeveiligingsbeleid en uitgebreid met het aandachtsgebied Privacy vanwege de ontwikkelingen van nieuwe wetgeving ten aanzien van bescherming van Persoonsgegevens in de Algemene Verordening Gegevensbescherming.

Beleid en verantwoording

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.

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.

De gemeente Nijmegen wil haar volwassenheidsniveau van de informatiebeveiliging verhogen. Zij streeft er naar om "in control" te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen via de Rapportage Informatiebeveiliging. In control betekent in dit verband dat de gemeente weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging. Zij weet welke (passende) maatregelen er genomen zijn en dat er een controleerbare planning is van de maatregelen die nog niet genomen zijn, die bewaakt moeten worden. Zij weet ook wat in hoeverre de maatregelen effectief zijn en welk risico er over blijft. Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is.

Uitgangspunten van de professionele gemeente Nijmegen

- Het informatiebeveiligingsbeleid van de gemeente Nijmegen is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving (AVG).
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de BIG.
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College van B&W van de gemeente Nijmegen. Het College van B&W herijkt periodiek het Informatiebeveiligingsbeleid. (De BIG hanteert minimaal 1x per 3 jaar. Momenteel wordt het beleid voor de 3de keer sinds 2015 herzien.)
- Het College van B&W van de gemeente Nijmegen is volgens de Wet bescherming persoonsgegevens (Wbp) de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. Het college ziet hier op toe.

Privacy

Als voorbereiding op de Algemene Verordening Gegevensbescherming (AVG), die vanaf mei 2018 van kracht zal worden, is in 2017 een Functionaris Gegevensbescherming (FG) gezocht alsook een Privacy Officer (PO). Ook is een start gemaakt met het bepalen van het Privacy beleid. Dit beleid zal in 2018 worden vastgesteld. 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

Algemeen Beeld en Resultaten

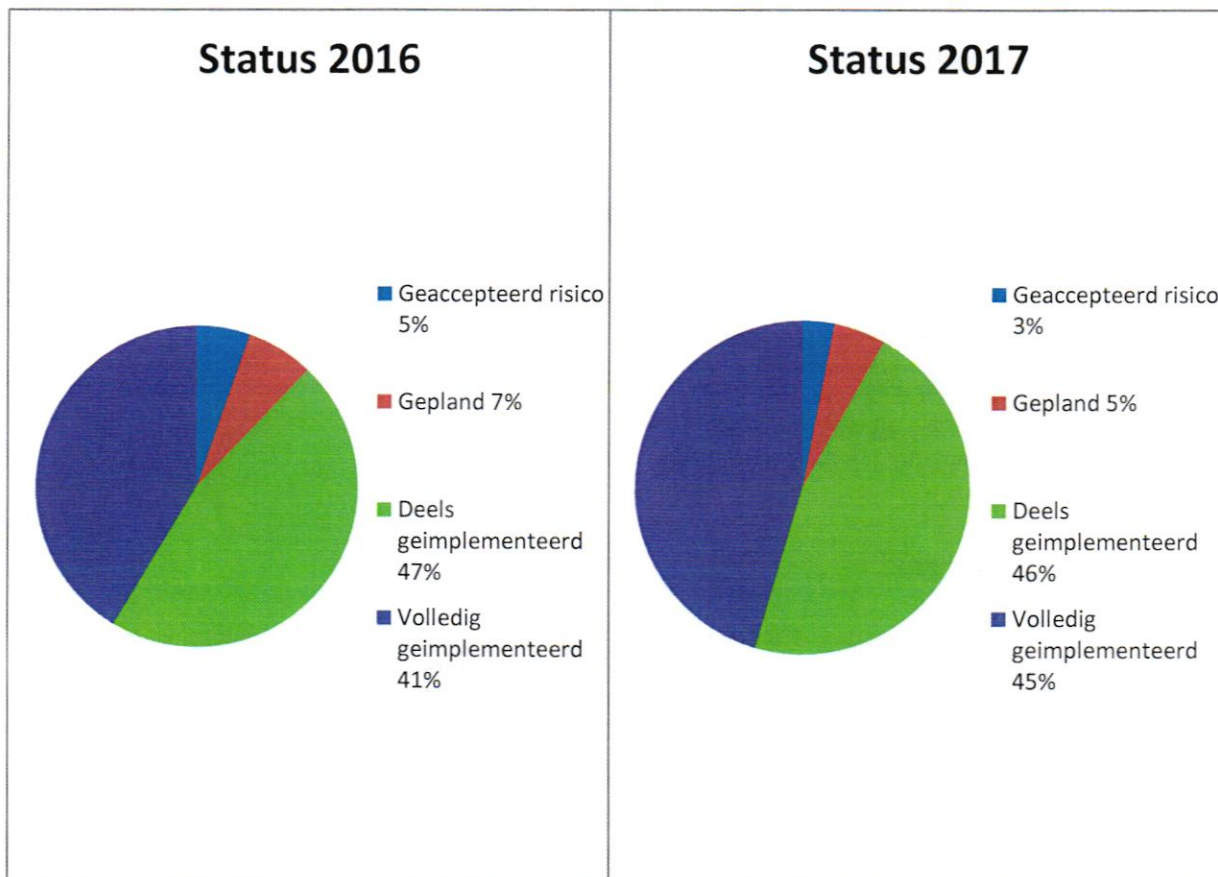
In de verantwoording over 2016 schreven wij dat in dat jaar veel aandacht gegaan is naar het vergroten van het informatiebewustzijn van de medewerkers. Het verhelderen van de verantwoordelijkheden van de medewerkers op het vlak van informatiebeveiliging was ook een punt van aandacht. In 2017 is veel aandacht besteed aan het inrichten van het achteraf controleren en analyseren van het gedrag van de medewerkers, en de toepassing van de beheersmaatregelen uit de BIG.

In 2017 zijn verdere stappen gezet op het punt van:

- Harmoniseren van informatiebeveiligingsbeleid: waar mogelijk en passend zijn bestaande beleidsdocumenten op het terrein van informatiebeveiliging samengevoegd om tot eenheid te komen in opzet, uitvoering en monitoring.
- Inbedden van checks & balances: In 2017 heeft de gemeente aandacht besteed aan het verder verbeteren van de organisatorische opzet en werking van de informatiebeveiliging. Er is onder meer een proef geweest met het inbedden van de controle op informatiebeveiligingsmaatregelen in de reguliere interne controle werkzaamheden; bijvoorbeeld om na te gaan of gepaste maatregelen zijn getroffen om de informatieveiligheid van persoonsgevoelige gegevens te garanderen.
- Aanstelling Functionaris Gegevensbescherming: Daarnaast is er in organisatorische zin een Functionaris Gegevensbescherming aangesteld.

Daarentegen heeft de iRvN vanwege de nadrukkelijke aandacht voor de continuïteit van haar dienstverlening tijdens de integratie van de omgevingen van de deelnemende gemeenten, niet de capaciteit gehad om de inrichting van de monitoring en de analyse op de informatiebeveiligingsmaatregelen af te ronden.

Naast de interne stappen die gezet zijn, in 2017 eveneens sprake geweest van een relevante externe ontwikkeling. Om de audit last voor de gemeenten te verlichten is vanuit het Ministerie van Binnenlandse Zaken namelijk het project ENSIA (Eenduidige Normatiek Single Information Audit) gestart. Hierbij wordt er een integrale omgeving beschikbaar gesteld aan gemeenten waarin zij een gemeentebrede zelfevaluatie op het vlak van informatiebeveiliging kunnen uitvoeren. Deze zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). Of we voldoen aan deze Baseline is getoetst door middel van de zelfevaluatie die is uitgevoerd in Q3 en Q4 2017. Om de zelfevaluatie goed uit te kunnen voeren wordt de status van de BIG maatregelen bijgehouden in een management systeem (ISMS). Hier komt ook de aanvullende informatie voor deze rapportage uit voort, zoals de samengevatte status van de maatregelen in de taartdiagrammen hier onder.



Aan de taartdiagrammen is te zien dat er een kleine vooruitgang geboekt is bij het implementeren van maatregelen. Dit betreft met name maatregelen op het vlak van sleutelbeheer, beperken van toegang tot informatie en maatregelen rond dataclassificatie. Ook op het vlak van mobiel werken, en de bedrijf continuïteit zijn ontwikkelingen in gang gezet.

Wij rapporteren nu als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid via ENSIA.

Vanuit de horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij de rijksoverheid afgeleid, de zogenaamde verticale verantwoording. Zo zijn de informatieveiligheidsvragen over de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN) per 1 oktober automatisch ingevoegd bij de kwaliteitsmonitor

voor verantwoording aan RvIG. Voor de Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Grootchalige Topografie (BGT) verantwoording worden de antwoorden in ENSIA automatisch naar het Ministerie van I&W opgeleverd. De onderliggende verantwoording voor BAG en BGT is bijgevoegd in een bijlage bij deze rapportage. De verantwoording over DigiD en SUWI is bijgevoegd bij de Collegeverklaring over deze twee stelsels.

Ten aanzien van de BAG wordt in de verantwoordingsrapportage het volgende gemeld: De huidige processen en werkafspraken leiden tot het goed, en in de meeste gevallen tijdig, registreren van de vergunde werkelijkheid. De koppelingen tussen de BAG en de BGT en tussen de BAG en de WOZ eisen in de komende jaren een kwaliteitsverbetering van het registreren van de feitelijke situatie. Ook terugmeldingen van belanghebbenden en van andere overheidsorganisaties eisen deze verbetering.

Ten aanzien van de BGT wordt de volgende conclusie getrokken:

De huidige capaciteit is niet voldoende om de kwaliteit goed te kunnen waarborgen. Er is in de laatste paar jaar een steeds grotere achterstand in actualiteit ontstaan, mede door de kaartconversie GBKN-BGT. In 2017 hebben we mede door het inzetten van inhuurkrachten wel achterstand ingelopen, maar we zijn nog niet actueel. Het beschikbare budget voor de BGT uit het gemeentefonds is niet toereikend om vóór 1 januari 2020 de BGT op geometrisch- en attributniveau voldoende actueel te hebben.

*Capaciteit
? Budget*

Voor het jaar 2017 geldt dat Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie en deze wordt getoetst door een IT auditor. Met de vastgestelde Collegeverklaring (inclusief de bijlagen over DigiD en Suwinet) en het Assurancerapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.

Voor 2018 staan verbetertrajecten gepland die de efficiëntie van de toetsing zullen vergroten. Deze rapportage is een onderdeel van de jaarcyclus rond informatiebeveiliging en zij is een verbreding en verdieping op de passage in de bedrijfsvoeringsparagraaf van het jaarverslag.

Beheersmaatregelen Informatiebeveiliging

Waar de voorgaande paragraaf een algemeen beeld geeft zoomt deze paragraaf meer in op de details en de verdeling van de verantwoordelijkheid.

Een overzicht van de belangrijkste maatregel categorieën die bijdragen aan het realiseren van de IB doelstellingen:

1. Cruciaal bij het implementeren van de BIG is het aanstellen van en CISO en het inrichten van het ISMS. Daarnaast is ook het hebben van een informatiebeveiligingsbeleid dat geactualiseerd wordt cruciaal.
2. Waar gemeenten samenwerken, bijvoorbeeld in verbonden partijen, moet duidelijk worden vastgelegd waar welke verantwoordelijkheid ligt. De risico's die ontstaan door het delen van omgevingen en informatie moeten worden beoordeeld en ondervangen.
3. Organisatorische maatregelen omvatten het beoordelen van overeenkomsten, het hebben van een goedkeuringsproces voor ICT-voorzieningen, het hanteren van geheimhoudingsovereenkomsten en het beoordelen van dienstverlening.
4. Het classificeren van informatie op het gebruik van persoons en het definiëren van geaccepteerd gebruik per classificatie.
5. Voor werknemers is het zaak te weten wat hun verantwoordelijkheden zijn. Ze dienen opgeleid te zijn om aan hun verantwoordelijkheden te kunnen voldoen. Het moet duidelijk zijn wat er verwacht wordt en wat er gebeurt als het mis gaat. Er moet scholing beschikbaar gesteld worden en documentatie.
6. Gebouwen, apparatuur en het netwerk moeten worden beveiligd tegen onbevoegd gebruik. Sleutels worden beheerd.

7. Aanpassingen aan systemen gebeuren gestructureerd en getest. Maatregelen tegen aanvallen worden gestructureerd genomen. Faciliteiten voor ontwikkeling, test en productie omgevingen zijn gescheiden.
8. Toegang tot applicaties en informatie wordt beperkt tot geautoriseerde personen. Het correcte niveau van toegang wordt afgedwongen. Netwerken zijn gescheiden en verkeer en gebruik wordt gemonitord.
9. De gegevens die in applicaties ingevoerd worden, en ook de uitvoer, worden gecontroleerd op correctheid.
10. Transport van gegevens is versleuteld. Opslag is ook versleuteld waar nodig.
11. Er wordt met grote regelmaat gezocht op kwetsbaarheden en deze worden zo snel mogelijk opgelost.
12. Er wordt gerapporteerd over de status van de informatiebeveiliging aan de CISO, de directie en aan het college. Maar ook richting de eigen organisatie (de lijn) en aan de rijksoverheid.
13. Het hebben van plannen die de continuïteit van informatiesystemen borgen. Het testen van de gemaakte plannen.
14. Weten welke wetgeving van toepassing is en de naleving daarvan kunnen aantonen aan auditors.

Concreet kan worden gesteld dat er in de afgelopen periode vooral gewerkt is aan de punten 1, 2, 4, 5 en 12. Punten 7, 8, 9, 10 en 11 liggen met name bij de iRvN. Punt 3 en punt 13 zullen in 2018 nog onderhanden genomen worden. Bewustwording (punt 5) is iets dat continue aandacht verdient om verlies van kennis en motivatie te voorkomen. Punt 14 is terug te vinden in de cyclus rond ENSIA. Dit overzicht maakt zichtbaar hoe breed het gebied is dat de informatiebeveiliging bestrijkt.

Maatregelen belegd bij de iRvN

Van de 133 beheersmaatregelen die onderdeel zijn van de BIG zijn de onderstaande 44 maatregelen toegekend aan de iRvN. Zoals boven aangegeven vallen deze in bepaalde gebieden. Deze maatregelen worden voor de bij de iRvN aangesloten gemeenten, de ODRN en de WBRN, op eenzelfde manier ingevuld. Van deze maatregelen gelden er 30 als volledig geïmplementeerd. Wel moet in 2018 de documentatie nog opgeleverd worden. Hier onder het overzicht van de maatregelen die bij de iRvN belegd zijn. De gemeente blijft eindverantwoordelijke en legt in die hoedanigheid ook over deze maatregelen verantwoording af.

Code	Maatregel	Code	Maatregel
6.1.4	Goedkeuringsproces voor ICT-voorzieningen	11.4.3	Identificatie van (netwerk)apparatuur
9.1.4	Bescherming tegen bedreigingen van buitenaf	11.4.4	Bescherming op afstand van poorten voor diagnose en configuraties
9.2.2	Nutsvoorzieningen	11.4.5	Scheiding van netwerken
9.2.3	Beveiliging van kabels	11.4.7	Beheersmaatregelen voor netwerkrouting
9.2.4	Onderhoud van apparatuur	11.5.1	Beveiligde inlogprocedures

9.2.6	Veilig verwijderen of hergebruiken van apparatuur	11.5.3	Systemen voor wachtwoordenbeheer
10.1.2	Wijzigingsbeheer	11.5.4	Gebruik van systeemhulpmiddelen
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	11.5.5	Time-out van sessies
10.3.1	Capaciteitsbeheer	11.5.6	Beperking van verbindingstijd
10.4.1	Maatregelen tegen virussen	11.6.1	Beperken van toegang tot informatie
10.4.2	Maatregelen tegen mobile code	11.6.2	Isoleren van gevoelige systemen
10.5.1	Reservekopien maken (back-ups)	11.7.1	Draagbare computers en communicatie-voorzieningen
10.6.1	Maatregelen voor netwerken	12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen
10.6.2	Beveiliging van netwerkdiensten	12.3.2	Sleutelbeheer
10.7.2	Verwijdering van media	12.4.1	Beheersing van operationele programmatuur
10.7.3	Procedures voor de behandeling van informatie	12.4.3	Toegangsbeheersing voor broncode van programmatuur
10.7.4	Beveiliging van systeemdokumentatie	12.5.1	Procedures voor wijzigingsbeheer
10.10.1	Aanmaken audit-logbestanden	12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
10.10.2	Controle van systeemgebruik	12.5.3	Restricties op wijzigingen in programmatuur
10.10.3	Bescherming van informatie in logbestanden	12.6.1	Beheersing van technische kwetsbaarheden
10.10.6	Synchronisatie van systeemklokken	15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen
11.4.2	Authenticatie van gebruikers bij externe verbindingen	15.2.2	Controle op technische naleving

Samenwerkingen

In het kader van het gastheerschap vult de gemeente Nijmegen voor de MGR en de ODRN een aantal maatregelen in, met name op het facilitaire en personeels vlak. Het betreft de volgende maatregelen:

In 2017 maakte de WBRN gebruik van de Suwinet aansluiting van gemeente Nijmegen. In 2018 zal de WBRN haar eigen aansluiting realiseren. De auditor 2Control heeft voor de regio

gemeenten die deelnemen aan de WBRN een verklaring afgegeven over het gebruik van deze aansluiting volgens de geldende normen.

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 heeft de auditor 2Control een verklaring afgegeven die de gemeente Mook en Middelaar in haar verantwoording zal gebruiken.

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.

Realisatie Doelstellingen

Sinds 1 januari 2016 is in Nederland de meldplicht datalekken in werking getreden. Er is sprake van een datalek als er als gevolg van een beveiligingsincident kans is op verlies of onrechtmatige verwerking van persoonsgegevens. Er wordt een registratie gevoerd, niet alleen van datalekken maar ook van beveiligingsincidenten. De meldplicht datalekken is bij elke workshop over informatiebeveiliging een belangrijk aandachtspunt.

In 2017 is het bewustzijn en de bereidheid tot melden toegenomen. Er zijn meer advies gesprekken geweest en in deze gesprekken is het belang van openheid en transparantie nadrukkelijker benoemd. In 2017 zijn 34 beveiligingsincidenten gemeld. Daarvan zijn er 6 gemeld bij de Autoriteit Persoonsgegevens. In 2016 zijn er 28 beveiligingsincidenten gemeld. Daarvan zijn er destijds 3 bij de Autoriteit Persoonsgegevens gemeld. De bereidheid tot melden is toegenomen doordat het bewustzijn toeneemt en het belang van transparantie nadrukkelijker benoemd wordt. In 2017 zijn de applicaties die gemeente Nijmegen gebruikt geclassificeerd op het belang van vertrouwelijkheid, integriteit, beschikbaarheid en duurzaamheid. Aan de classificatie van een applicatie hangen gevolgen voor de beschermende maatregelen. Deze maatregelen zullen gerealiseerd moeten worden om compliant te zijn aan de BIG. Ook zal hier op toegezien moeten worden. In 2017 zijn de mogelijkheden tot toetsing toegenomen.

Toetsing vindt plaats middels de Zelfevaluatie Informatiebeveiliging (ENSIA). Hier van worden meer aspecten ge-audit dan in 2016. Toetsing door interne controle zal in de loop van 2018 worden opgezet.

In 2017 is bij de MGR een CISO aangesteld. Dit verschaft meer duidelijkheid omtrent de wederzijdse verantwoordelijkheden. Ook aan de kant van de gemeente.

Meerjaren Perspectief

Informatiebeveiliging

In 2018 krijgt de nieuwe opzet van Stadscontrol vorm. Informatiebeveiliging en privacy vormen hier een essentieel onderdeel van. In de komende jaren zullen de interne controle mechanismen ook toegepast worden op de toetsing van informatiebeveiligingsmaatregelen. Ook zal er regionaal een "collegiaal audit circuit" opgezet worden zodat er altijd een vinger aan de pols gehouden wordt. Door er voor te zorgen dat er continu een beeld bestaat van hoe we er voor staan op het vlak van informatiebeveiliging wordt het gemakkelijker om verbeter trajecten op te zetten en af te ronden. Ook waar het gaat om het toe zien op de informatiebeveiliging in samenwerkingsverbanden zal het "collegiaal auditen" een belangrijk hulpmiddel zijn.

Wat de ontwikkelingen zullen zijn op het vlak van ENSIA is niet bekend. De verwachting is 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. Dit 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.

Bewustwording blijft een onderwerp waarop veel geïnvesteerd moet worden om de benodigde cultuuromslag te bewerkstelligen. In de eerste 2 maanden van 2018 zijn er 6 incidenten gemeld.

Opvallend is dat het bewustzijn bij bepaalde organisatie onderdelen hoger is dan bij anderen. De cultuuromslag is ook benodigd om als organisatie meer op een lijn te komen. 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 DigiD 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. 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.

Privacy

Het aanstellen van de Privacy Officer begin 2018 zorgt er voor dat er meer aandacht naar het onderwerp privacy en daarmee ook informatiebeveiliging gaat. In de komende periode zal de aandacht uit gaan naar het creëren van bewustzijn, het op orde brengen van de registers (verwerkingen, datalekken, inzageverzoeken) en de procedures om de rechten van de betrokkenen te borgen. Ook zal er geborgd worden dat bij de gevoelige verwerkingen, die middels de dataclassificatie in beeld zijn gebracht, PIA's zijn en worden afgenomen. De PIA's worden, net als de verwerkersovereenkomsten actief geregistreerd. Dit betekent dat centraal contractmanagement nodig is, en met voorrang moet worden ingevoerd. In 2018 wordt een CISO/FG bij de ODRN aangesteld. Geleidelijk aan nemen steeds meer partners van de gemeente hun verantwoordelijkheid en worden de onderlinge relaties gedefinieerd.

Dubbele
functie?

Rapportage Informatiebeveiliging en Privacy



Periode 2018

Inhoud

Rapportage	1
Informatiebeveiliging en Privacy	1
Verspreiding	3
Doel en scope	4
Beleid en verantwoording	4
Informatiebeveiliging	4
Privacy	5
Algemeen Beeld en Resultaten	5
Beheersmaatregelen Informatiebeveiliging	8
Aanpak Privacy	9
Maatregelen belegd bij de iRvN	10
Samenwerkingen	11
Realisatie Doelstellingen	12
Meerjaren Perspectief	13
Informatiebeveiliging	13
Privacy	13

Verspreiding

De rapportage wordt opgesteld door de CISO, vastgesteld door het college en ter kennisname verstuurd aan directie en met een begeleidende brief aangeboden aan B&W. Het verslag bij de jaarrekening bevat in de paragraaf over bedrijfsvoering een passage over informatiebeveiliging en privacy. Dit document wordt via de website <http://pcportal.nijmegen.nl/> gepubliceerd. De rapportage die voor u ligt is een verdieping en verbreding op de passage in het jaarverslag.

Doel en scope

Gemeenten hebben in de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' van november 2013 onder meer afgesproken dat in het jaarverslag een aparte paragraaf over informatiebeveiliging wordt opgenomen. Dit is een van de maatregelen van het normenkader Baseline Informatiebeveiliging Gemeenten (BIG). Met deze paragraaf verantwoordt het college van B&W zich aan de gemeenteraad over informatiebeveiliging in brede zin. De separate jaarrapportage die hier voor ligt bevat de ontwikkelingen, activiteiten, incidenten en risico's met betrekking tot de onderwerpen informatieveiligheid en privacy bij de gemeente Nijmegen over het jaar 2018. Het geeft de ruimte om een beeld te schetsen van de ontwikkeldoelen voor de komende periode en de bedreigingen die van invloed zijn of kunnen zijn op de gemeente. De rapportage is in overeenstemming met het door het college vastgestelde informatiebeveiligingsbeleid, en uitgebreid met het aandachtsgebied Privacy vanwege de ontwikkelingen van nieuwe wetgeving ten aanzien van bescherming van Persoonsgegevens in de Algemene Verordening Gegevensbescherming.

Beleid en verantwoording

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 van 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.

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.

De gemeente Nijmegen wil haar volwassenheidsniveau van de informatiebeveiliging verhogen. Zij streeft er naar om "in control" te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen via de Rapportage Informatiebeveiliging. In control betekent in dit verband dat de gemeente weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging. Zij weet welke (passende) maatregelen er genomen zijn en dat er een controleerbare planning is van de maatregelen die nog niet genomen zijn, die bewaakt moeten worden. Zij weet ook in hoeverre de maatregelen effectief zijn en welk risico er over blijft. Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is.

Uitgangspunten van de professionele gemeente Nijmegen

- Het informatiebeveiligingsbeleid van de gemeente Nijmegen is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving (Uitvoeringswet) AVG.
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de BIG. Vanaf 2020 de BIO.
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College van B&W van de gemeente Nijmegen. Het College van B&W herijkt periodiek het Informatiebeveiligingsbeleid. (De BIG hanteert minimaal 1x per 3 jaar. Momenteel wordt het beleid jaarlijks herzien.)
- Het College van B&W van de gemeente Nijmegen is volgens de Algemene Verordening Gegevensbescherming de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. Het college ziet hier op toe.

Privacy

De (uitvoeringswet) Algemene Verordening Gegevensbescherming (AVG), is 25 mei 2018 van kracht geworden. Er is in 2017 een Functionaris Gegevensbescherming (FG) aangesteld alsook een Privacy Officer (PO). Ook is het Privacy beleid in afstemming met het informatiebeveiligingsbeleid in 2018 vastgesteld. 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

Een aantal maatregelen die tot doel hebben de transparantie te vergroten, zijn in 2018 ingevoerd. Het goed inzetten van de beschikbare informatie om de organisatie te professionaliseren is een kernpunt in het jaarplan van Stadscontrol. Dit vertaalt zich in eerste instantie in een focus op iBewustzijn, processen en technische maatregelen.

Algemeen Beeld en Resultaten

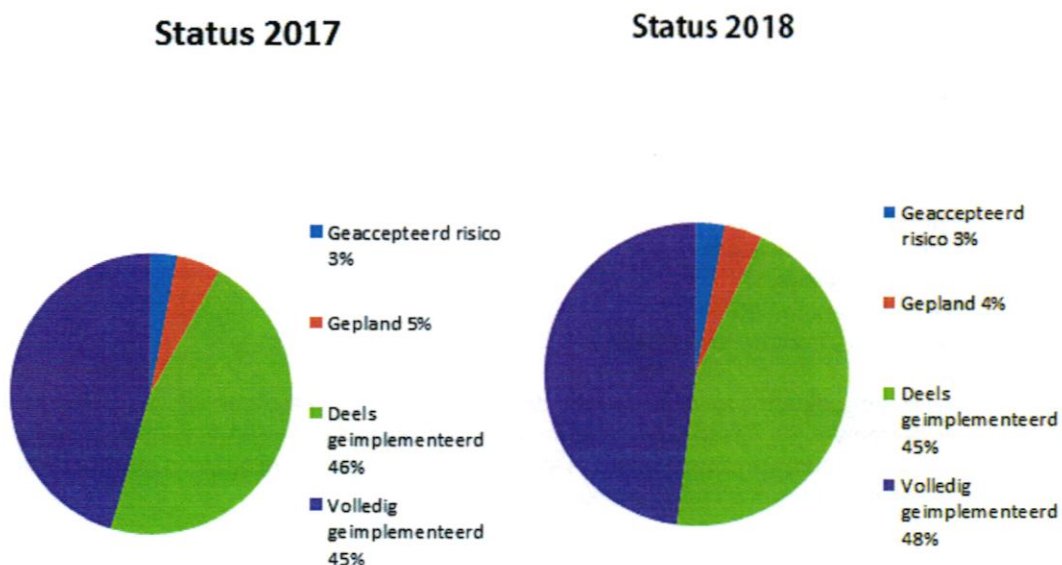
In de verantwoording over 2017 schreven wij dat in dat jaar veel aandacht gegaan is naar het harmoniseren van het Informatiebeveiligingsbeleid, het uitvoeren van interne controle op persoonsgegevens en het aanstellen van een Functionaris Gegevensbescherming. In 2018 is veel aandacht besteed aan het inrichten van de rol van de Functionaris Gegevensbescherming, de Privacy Officer en het kenniscluster Privacy en informatiebeveiliging. Daarnaast is veel aandacht geweest voor het structureel inbedden van de AVG in de gemeentelijke organisatie. Alsmede is voldaan aan de verplichte onderwerpen van de AVG. Bovendien is er veel energie uitgegaan naar de inrichting van Stadscontrol als manier om de volwassenheid van de organisatie te vergroten.

In 2018 zijn verdere stappen gezet op het punt van:

- Harmoniseren van informatiebeveiligingsbeleid, met name voor het SUWI stelsel, waar mogelijk en passend zijn bestaande beleidsdocumenten op het terrein van informatiebeveiliging samengevoegd om tot eenheid te komen in opzet, uitvoering en monitoring.
- Inbedding Functionaris Gegevensbescherming/CISO bij Stadscontrol. Om de onafhankelijkheid van de CISO en FG rollen te vergroten zijn deze ondergebracht in een staf bureau "Stadscontrol".

De iRvN heeft in het afgelopen jaar de robuustheid van haar dienstverlening door middel van de integratie van de omgevingen van de deelnemende gemeenten en het verbeteren van de infrastructuur kunnen verstevigen. Het ging hier met name om het verbeteren van het netwerk en het scannen op kwetsbaarheden.

In 2017 is de eerste ENSIA cyclus afgerond. Om de audit last voor de gemeenten te verlichten is vanuit het Ministerie van Binnenlandse Zaken het project ENSIA (Eenduidige Normatiek Single Information Audit) gestart. Hierbij is in 2017 een integrale omgeving beschikbaar gesteld aan gemeenten waarin zij een gemeentebrede zelfevaluatie op het vlak van informatiebeveiliging kunnen uitvoeren. Deze zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). Of we voldoen aan deze Baseline is getoetst door middel van de zelfevaluatie die is uitgevoerd in Q3 en Q4 2018. Om de zelfevaluatie goed uit te kunnen voeren wordt de status van de BIG maatregelen bijgehouden in een management systeem (ISMS). Hier komt ook de aanvullende informatie voor deze rapportage uit voort, zoals de samengevatte status van de maatregelen in de taartdiagrammen hier onder.



Aan de taartdiagrammen is te zien dat er een **kleine vooruitgang geboekt is bij het implementeren van maatregelen**. Dit betreft met name maatregelen op het vlak van netwerkbeheer, en het voeren van registraties. Verdere ontwikkelingen op het vlak van professionalisering worden doorgevoerd, al wordt er op het vlak van beveiliging ook met sommige initiatieven gewacht op de aanbesteding van GGI Veilig.

Wij rapporteren nu als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid via ENSIA.

Vanuit de horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij de rijksoverheid afgeleid, de zogenaamde verticale verantwoording. Zo zijn de informatieveiligheidsvragen over de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN) per 31 december (hier voor 1 oktober) automatisch ingevoegd bij de kwaliteitsmonitor voor verantwoording aan RvIG. Voor de Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Grootchalige Topografie (BGT) verantwoording worden de antwoorden in ENSIA automatisch naar het Ministerie van I&W opgeleverd. De onderliggende verantwoording voor BAG en BGT is aan het college aangeboden

in een bijlage bij de Collegeverklaring ENSIA 2018. De verantwoording over DigiD en SUWI is bijgevoegd bij de Collegeverklaring ENSIA 2018, over deze twee stelsels.

Ten aanzien van de BAG wordt in de verantwoordingsrapportage het volgende gemeld: De huidige processen en werkafspraken leiden tot het goed, en in de meeste gevallen tijdig, registreren van de vergunde werkelijkheid. Een nieuw proces is ingevoerd in 2018 waarbij BAG-objecten ook gereed gemeld worden door een inschrijving op het adres in het Handelsregister of de Basisregistratie Personen. De koppelingen tussen de BAG en de BGT en tussen de BAG en de WOZ eisen in de komende jaren een kwaliteitsverbetering van het registreren van de feitelijke situatie. Veel werk gaat het nog kosten om de gebruiksovervlaktes te berekenen. Voor alle woningen moet dit 1-1-2022 gereed zijn. De afspraak met het bureau Gemeentebelastingen is gemaakt om deze berekeningen te maken. De capaciteit is hiervoor onvoldoende. Dit knelpunt staat verwoord in de ENSIA BAG-rapportage van 2018.

Een ander vraagstuk is de koppeling van de BAG aan het gemeentelijk Handhavingsbeleid: vanuit de wet BAG registreren we ook objecten (panden en verblijfsobjecten) die zonder de juiste WABO-vergunning zijn gebouwd. De planning is om in 2019 het Handhavingsbeleid voor deze situaties uit te werken.

Ten aanzien van de BGT wordt de volgende conclusie getrokken:

De formatie is voldoende voor het reguliere werk en de pieken worden uitbesteed. De vervanging voor het BGT beheer proces is gewaarborgd. Door middel van cursussen blijft de kennis op pijl en er is periodiek inhoudelijk overleg. Aan de actualiteit wordt gewerkt. Nieuwe mutaties in de topografie worden op tijd verwerkt in de BGT. Momenteel wordt de bebouwing aan de achterzijde van de hoofdbebouwing geactualiseerd met behulp van luchtfoto's. Dit zijn veelal ook BAG-panden die vergunningsvrij zijn gebouwd. Hiervoor is in 2018 veel werk verzet. Na inwinning wordt de geometrie door gestuurd naar de BAG. In de BGT is hiervan zo'n 40% verwerkt. Het streven is dit gereed te hebben in het najaar van 2019. De meldingen die gedaan zijn in het landelijke MMS zijn voor een groot deel verwerkt. Het beschikbare budget voor de BGT uit het gemeentefonds is niet toereikend om vóór 1 januari 2020 de BGT op geometrisch- en attributniveau voldoende actueel te hebben.

Ten aanzien van Suwinet en DigiD geldt het volgende: Voor het jaar 2018 geldt dat Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie en deze wordt getoetst door een IT auditor. De gemeente voldoet, zo meldt zij in de verklaring, met de maatregelen die er getroffen zijn aan de relevante normen. Met de vastgestelde Collegeverklaring (inclusief de bijlagen over DigiD en Suwinet) en het Assurancerapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD. De efficiëntie van het verantwoordingsproces zelf is voor verbetering vatbaar. Voor 2019 zijn hier afspraken over gemaakt.

Voor 2019 wordt in januari het implementatieplan iBewustzijn gepresenteerd samen met het voorstel over eigenaarschap. Dit zal betekenen dat het initiatief en de verantwoording daar belegd zal worden waar hij thuis hoort. Stadscontrol zal deze stap monitoren en toetsen, en waar nodig begeleiden. Deze rapportage is een onderdeel van de jaarcyclus rond informatiebeveiliging en zij is een verbreding en verdieping op de passage in de bedrijfsvoeringsparagraaf van het jaarverslag.

Beheersmaatregelen Informatiebeveiliging

Waar de voorgaande paragraaf een algemeen beeld geeft zoomt deze paragraaf meer in op de details en de verdeling van de verantwoordelijkheid.

Een overzicht van de belangrijkste maatregel categorieën die bijdragen aan het realiseren van de IB doelstellingen:

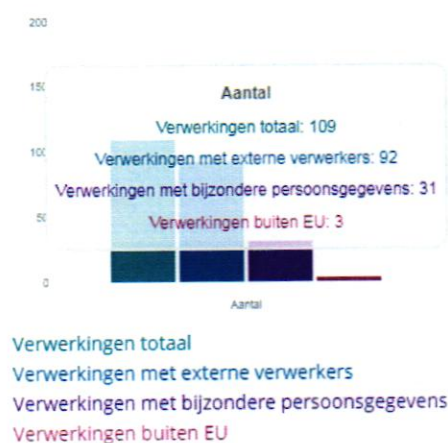
1. Cruciaal bij het implementeren van de BIG is het **aanstellen van en CISO en het inrichten van het ISMS**. Daarnaast is ook het hebben van een **informatiebeveiligingsbeleid dat geactualiseerd** wordt cruciaal.
2. Waar **gemeenten samenwerken**, bijvoorbeeld in verbonden partijen, moet duidelijk worden vastgelegd **waar welke verantwoordelijkheid ligt**. De risico's die ontstaan door het delen van omgevingen en informatie moeten worden beoordeeld en ondervangen.
3. **Organisatorische maatregelen** omvatten het beoordelen van overeenkomsten, het hebben van een goedkeuringsproces voor ICT-voorzieningen, het hanteren van geheimhoudingsovereenkomsten en het beoordelen van dienstverlening.
4. Het **classificeren** van informatie op het gebruik van persoonsgegevens en het definiëren van geaccepteerd gebruik per classificatie.
5. Voor **werknemers** is het zaak te weten wat hun **verantwoordelijkheden** zijn. Ze dienen **opgeleid te zijn** om aan hun verantwoordelijkheden te kunnen voldoen. Het moet duidelijk zijn wat er verwacht wordt en wat er gebeurt als het mis gaat. Er moet scholing beschikbaar gesteld worden en documentatie.
6. Gebouwen, apparatuur en het netwerk moeten worden **beveiligd tegen onbevoegd gebruik**. Sleutels worden beheerd.
7. **Aanpassingen aan systemen gebeuren gestructureerd en getest**. Maatregelen tegen aanvallen worden gestructureerd genomen. Faciliteiten voor ontwikkeling, test en productie omgevingen zijn gescheiden.
8. **Toegang tot applicaties en informatie wordt beperkt tot geautoriseerde personen**. Het correcte niveau van toegang wordt afgedwongen. Netwerken zijn gescheiden en verkeer en gebruik wordt gemonitord.
9. De **gegevens die in applicaties ingevoerd worden**, en ook de uitvoer, worden **gecontroleerd op correctheid**.
10. Transport van gegevens is **versleuteld**. Opslag is ook versleuteld waar nodig.
11. Er wordt met grote regelmaat **gezocht op kwetsbaarheden** en deze worden zo snel mogelijk opgelost.
12. Er wordt **gerapporteerd over de status van de informatiebeveiliging aan de CISO, de directie en aan het college**. Maar ook richting de eigen organisatie (de lijn) en aan de rijksoverheid.
13. Het hebben van plannen die de **continuïteit van informatiesystemen borgen**. Het testen van de gemaakte plannen.
14. Weten welke **wetgeving van toepassing is** en de naleving daarvan kunnen aantonen aan auditors.

Concreet kan worden gesteld dat er na het begin met het aanstellen van de CISO, er in het afgelopen jaar gewerkt is aan de punten 2, 4, 5 en 12. Punten 7, 8, 9, 10 en 11 liggen met name bij de iRvN. Punt 3 en punt 13 zullen in 2019 nog onderhanden genomen worden. Bewustwording (punt 5) is iets dat continue aandacht verdient om verlies van kennis en motivatie te voorkomen. In 2018 is hier met name aandacht voor geweest in adviesgesprekken en onderzoeken. Punt 14 is terug te vinden in de cyclus rond ENSIA. Daarnaast is het niet zo dat eenmaal uitgevoerde punten geen aandacht meer nodig hebben. Ook punt 4 zal in 2019 herzien moeten worden (ook vanuit de BIO), net als punt 2, vanwege veranderingen die plaats vinden. Dit overzicht maakt zichtbaar hoe breed het gebied is dat de informatiebeveiliging bestrijkt.

Aanpak Privacy

Op het vlak van het treffen van maatregelen om de bescherming van de persoonsgegevens van burgers en medewerkers te waarborgen, en daarmee aan de privacy wetgeving te voldoen, zijn een aantal maatregelen getroffen. De aanstelling van de FG en de Privacy Officer zijn een eerste cruciale stap. Daarna is er een Verwerkingenregister ingericht. Op dit moment zijn er van 109 verwerkingen 38 bijpassende overeenkomsten beschikbaar. Daarnaast zijn er een groot aantal conceptovereenkomsten aan leveranciers gezonden in afwachting van ondertekening. Het is bemoedigend dat het aantal registraties met geldige overeenkomsten stijgt. Omdat inkopen decentraal gebeurt vraagt het een hoge mate van bewustzijn om elke verwerking in het systeem opgenomen te krijgen. Het verwerkingenregister wordt het kader van het manifest 'Open en Weerbaar' gepubliceerd. Het publiceren van het register van verwerkingen is overigens geen wettelijke verplichting.

Verwerkingen



Overeenkomsten



Figuur 1 De situatie in 2018

Burgers kunnen in het kader van de AVG een aantal rechten uitoefenen, zoals het recht op inzage in welke gegevens de gemeente van hen verwerkt. In 2018 zijn er 14 verzoeken ingediend bij de gemeente. Deze zijn op een na allemaal binnen de termijn afgehandeld. Daarnaast worden datalekken geregistreerd. Over 2018 zijn er zo'n 40 mogelijke datalekken gemeld. Hiervan zijn er 7 gemeld bij de AP. Dit zijn de gevallen die feitelijk een datalek met groot risico op een inbreuk op de persoonlijke levenssfeer blijken te zijn. De resterende 33 situaties zijn beveiligingsincidenten, variërend van versleutelde verloren telefoons, inloggen onder het account van iemand anders, tot situaties waarbij data door de verkeerde afdeling is ingezien, en situaties waarin de gemeente niet de verantwoordelijke is.

Jaar	Beveiligingsincidenten	Gemeld bij AP
2016	28	3
2017	34	6
2018	40	7

De zichtbaarheid van het kenniscluster Privacy en Informatiebeveiliging, de CISO en de FG nemen nog steeds toe. Dit komt door enerzijds door de toenemende bewustwording en

positionering van het privacyrecht onder medewerkers en anderzijds door de nieuwe inrichting van Stadscontrol. Dit betekent dat er meer mogelijke problemen actief aangekaart worden en er problemen gesignaleerd worden.

Vanuit de dataclassificatie worden maatregelen genomen om de applicaties met gevoelige gegevens beter te beschermen. Dit begint met het uitvoeren van DPIA's op deze verwerkingen. In 2018 is een start gemaakt met het standaard uitvoeren van DPIA's bij nieuwe verwerkingen, en met terugwerkende kracht over gevoelige al bestaande verwerkingen. Dit betreft verwerkingen die bovenaan de hiërarchie in de dataclassificatie staan. In 2018 was er met name aandacht voor het datawarehouse. Daarnaast waren er nog 2 DPIA's. In 2019 ligt de focus bij Corsa. De DPIA van deze applicatie is in Q1 van 2019 afgerond.

Maatregelen belegd bij de iRvN

Van de 133 beheersmaatregelen die onderdeel zijn van de BIG zijn de onderstaande 44 maatregelen toegekend aan de iRvN. Zoals boven aangegeven vallen deze in met name technische gebieden, zoals netwerkbeveiliging, versleuteling en systeem toegang en logging. Deze maatregelen worden voor de bij de iRvN aangesloten gemeenten, de ODRN en de WBRN, op eenzelfde manier ingevuld. Van deze maatregelen gelden er 30 als volledig geïmplementeerd. Wel moet in 2019 nog een deel van de documentatie nog opgeleverd worden. Hier onder het overzicht van de maatregelen die bij de iRvN belegd zijn. Met name op het vlak van de inrichting van het netwerk zijn in 2018 stappen gezet. In 2019 zal GGI Veilig worden aanbesteed en ook gegund. Daarmee zullen verdere maatregelen op het vlak van bijvoorbeeld SIEM en MDM worden gerealiseerd. De gemeente blijft eindverantwoordelijke en legt in die hoedanigheid ook over deze maatregelen verantwoording af.

Code	Maatregel	Code	Maatregel
6.1.4	Goedkeuringsproces voor ICT-voorzieningen	11.4.3	Identificatie van (netwerk)apparatuur
9.1.4	Bescherming tegen bedreigingen van buitenaf	11.4.4	Bescherming op afstand van poorten voor diagnose en configuraties
9.2.2	Nutsvoorzieningen	11.4.5	Scheiding van netwerken
9.2.3	Beveiliging van kabels	11.4.7	Beheersmaatregelen voor netwerkroutering
9.2.4	Onderhoud van apparatuur	11.5.1	Beveiligde inlogprocedures
9.2.6	Veilig verwijderen of hergebruiken van apparatuur	11.5.3	Systemen voor wachtwoordenbeheer
10.1.2	Wijzigingsbeheer	11.5.4	Gebruik van systeemhulpmiddelen
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	11.5.5	Time-out van sessies
10.3.1	Capaciteitsbeheer	11.5.6	Beperking van verbindingstijd

10.4.1	Maatregelen tegen virussen	11.6.1	Beperken van toegang tot informatie
10.4.2	Maatregelen tegen mobile code	11.6.2	Isoleren van gevoelige systemen
10.5.1	Reserve kopieën maken (back-ups)	11.7.1	Draagbare computers en communicatie-voorzieningen
10.6.1	Maatregelen voor netwerken	12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen
10.6.2	Beveiliging van netwerkdiensten	12.3.2	Sleutelbeheer
10.7.2	Verwijdering van media	12.4.1	Beheersing van operationele programmatuur
10.7.3	Procedures voor de behandeling van informatie	12.4.3	Toegangsbeheersing voor broncode van programmatuur
10.7.4	Beveiliging van systeemdokumentatie	12.5.1	Procedures voor wijzigingsbeheer
10.10.1	Aanmaken audit-logbestanden	12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
10.10.2	Controle van systeemgebruik	12.5.3	Restricties op wijzigingen in programmatuur
10.10.3	Bescherming van informatie in logbestanden	12.6.1	Beheersing van technische kwetsbaarheden
10.10.6	Synchronisatie van systeemklokken	15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen
11.4.2	Authenticatie van gebruikers bij externe verbindingen	15.2.2	Controle op technische naleving

Samenwerkingen

In het kader van het gastheerschap vult de gemeente Nijmegen voor de MGR en de ODRN een aantal maatregelen in, met name op het vlak van facilitair en personeel. Het betreft maatregelen die te maken hebben met voorzieningen op het gebied van facilitair, personeel en juridische zaken.

Dit omvat onder andere maatregelen op het vlak van contractbeheer, toegangsbeleid en telewerken:

6.2.1 en 6.2.3	Omgaan met derden
7.1.2 en 7.1.3	Eigenaarschap van bedrijfsmiddelen
7.2.1. en 7.2.2	Verwerking van informatie
8.1.1 en 8.2.2	Verantwoordelijkheden en bewustwording
8.3.1, 8.3.2 en 8.3.3	Beëindiging dienstverband
9.1.1 – 9.1.6	Fysieke toegang
10.1.1	Documentatie van procedures
10.2.2 en 10.2.3	Toetsing van derden
10.3.2	Systeemacceptatie

10.7.1. en 10.7.4	Verwijderbare media en systeemdokumentatie
10.8.1 -10.8.5	Informatie uitwisseling
10.9.2 en 10.9.3	Online transacties
10.10.1 – 10.10.6	Logbestanden
11.1.1	Toegangsbeleid
11.2.1,11.2.2. en 11.2.4,	
11.3.1 en 11.3.2	Wachtwoorden en gebruikersapparatuur
11.4.1,11.4.2 en 11.4.6	Netwerkverbindingen
11.5.2	Identificatie en authenticatie
11.7.2	Telewerken
12.1.1	Analyse en specificatie
12.2.1,12.2.2 en 12.2.3	Interne gegevensverwerking
12.4.2	Test data
12.5.4 en 12.5.5	Datalekken en software ontwikkeling
13.2.3	Bewijsmateriaal
14.1.1 – 14.1.5	Bedrijfscontinuïteit
15.1.2,15.1.3 en 15.1.5	Bescherming van intellectueel eigendom en voorkomen van misbruik
15.3.1 en 15.3.2	Beheer van audits

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 de WBRN de beschikking gekregen over haar eigen Suwinet aansluiting. De auditor 2Control zal voor de regio gemeenten die deelnemen aan de WBRN een verklaring afgeven over het gebruik van de Suwinet aansluiting volgens de geldende normen. 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 heeft de auditor 2Control een verklaring afgeven die de gemeente Mook en Middelaar in haar verantwoording zal gebruiken.

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. Het nieuwe bureau Stadscontrol zal hier in 2019 in het kader van de sturing op externe relaties aandacht aan besteden.

Realisatie Doelstellingen

Op 1 januari 2016 is in Nederland de meldplicht datalekken in werking getreden. Er is sprake van een datalek als er als gevolg van een beveiligingsincident kans is op verlies of onrechtmatige verwerking van persoonsgegevens. Er wordt een registratie gevoerd, niet alleen van datalekken maar ook van beveiligingsincidenten. De meldplicht datalekken is bij elke workshop over informatiebeveiliging een belangrijk aandachtspunt.

In 2018 is het bewustzijn en de bereidheid tot melden verder toegenomen. Er zijn meer advies gesprekken geweest en in deze gesprekken is het belang van openheid en transparantie nadrukkelijker benoemd. In 2018 zijn meer beveiligingsincidenten gemeld dan in 2017. Daarvan is er 1 meer gemeld bij de Autoriteit Persoonsgegevens. De bereidheid tot melden is toegenomen doordat het bewustzijn toeneemt en het belang van transparantie nadrukkelijker benoemd wordt in de context van de Open en Weerbaar campagne van gemeente Nijmegen.

In 2017 zijn de applicaties die gemeente Nijmegen gebruikt geclassificeerd op het belang van vertrouwelijkheid, integriteit, beschikbaarheid en duurzaamheid. Aan de classificatie van een applicatie hangen gevolgen voor de beschermende maatregelen. Deze maatregelen zullen gerealiseerd moeten worden om compliant te zijn aan de BIG. Ook zal hier op toegezien moeten worden. In 2018 zijn de mogelijkheden tot toetsing toegenomen door de inburgering van het instrument, de DPIA en het kenniscluster Privacy en informatiebeveiliging.

Integrale toetsing vindt plaats middels de Zelfevaluatie Informatiebeveiliging (ENSIA). Een aantal vragen zijn veranderd ten opzichte van de vragenlijst van 2017 zodat er meer gericht doorgevraagd wordt. Toetsing door interne controle zal in de loop van 2019 door het nieuwe Stadscontrol worden opgezet.

Ook het iRvN en de WBRN werken aan professionalisering.

Meerjaren Perspectief

Informatiebeveiliging

In 2018 is het Jaarplan 2019 van Stadscontrol gepresenteerd. Informatiebeveiliging en privacy vormen hier een essentieel onderdeel van. In het jaarplan wordt beschreven welke initiatieven er in 2019 zullen worden opgepakt. Het ondersteunen van en bijdragen aan initiatieven op het vlak van iBewustzijn spelen een centrale rol. In de komende jaren zullen de interne controle mechanismen ook toegepast worden op de toetsing van informatiebeveiligingsmaatregelen. Er zal intern en regionaal een "collegiaal audit circuit" opgezet worden zodat er altijd een vinger aan de pols gehouden wordt. Door er voor te zorgen dat er continu een beeld bestaat van hoe we er voor staan op het vlak van informatiebeveiliging wordt het gemakkelijker om verbeter trajecten op te zetten en af te ronden. Ook waar het gaat om het toe zien op de informatiebeveiliging in samenwerkingsverbanden en bij leveranciers zal het "collegiaal auditen" een belangrijk hulpmiddel zijn.

Wat de ontwikkelingen zullen zijn op het vlak van ENSIA is niet in detail 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. Naar het zich laat aanzien zal dit in 2020 gebeuren. Op dit moment beperkt de toetsing zich tot opzet en bestaan. De ontwikkelingen zullen de volwassenheid van de gemeente Nijmegen ten goede komen. Dergelijke ontwikkelingen zullen ook gevolgen hebben voor de eisen die wij stellen aan de partijen waar wij mee samen werken. Bewustwording blijft een onderwerp waarop veel geïnvesteerd moet worden om de benodigde cultuuromslag te bewerkstelligen. Opvallend is dat het bewustzijn bij bepaalde organisatie onderdelen hoger is dan bij anderen. De cultuuromslag is ook benodigd om als organisatie meer op een lijn te komen.

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 DigiD 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.

Privacy

Het aanstellen van de Privacy Officer en Functionaris voor Gegevensbescherming begin 2018, de positionering van de afdeling Stadscontrol en het kenniscluster Privacy en Informatiebeveiliging met leden vanuit het fysiek- en sociaaldomein zorgt er voor dat er meer aandacht en bewustzijn naar het onderwerp privacy en daarmee ook informatiebeveiliging gaat. In de komende periode zal de aandacht uit gaan naar het creëren van bewustzijn, het vervullen van de registers (verwerkingen, datalekken, inzageverzoeken) en de procedures om de rechten van de

betrokkenen duurzaam binnen de organisatie te borgen. Ook zal er geborgd worden dat bij de gevoelige verwerkingen (middel en hoogrisico), die middels de dataclassificatie in beeld zijn gebracht, DPIA's zijn en worden afgenomen. De DPIA's worden, net als de verwerkersovereenkomsten actief geregistreerd. Hiermee wordt onder andere voldaan aan de verantwoordingsplicht vanuit de AVG. Centraal contractmanagement is niet beschikbaar, daarom moeten er andere waarborgen worden ingevoerd. Het afwegen en invoeren van alternatieve maatregelen en waarborgen vraagt een brede discussie. Bewustzijn van de risico's en de urgentie is hier bij nodig.

Rapportage Informatiebeveiliging en Privacy

Periode 2019



Inhoud

Rapportage	1
Informatiebeveiliging en Privacy	1
Periode 2019	1
Verspreiding	3
Doel en scope	4
Beleid en verantwoording	4
Informatiebeveiliging	4
Privacy	5
Algemeen Beeld en Resultaten	5
Huidige Stand	5
Resultaat Informatiebeveiliging	9
Resultaat Privacy	10
Samenwerkingen	12
Maatregelen belegd bij de iRvN	12
Andere Samenwerkingen	13
Doelstelling gemeente Nijmegen	14
Realisatie	14
Evaluatie	15
Perspectief	15
Plan voor 2020	15
Meerjarenvoorzicht Informatiebeveiliging	16
Meerjarenvoorzicht Privacy	16

Verspreiding

De rapportage wordt opgesteld door de CISO en de FG, vastgesteld door het college en ter kennisname verstuurd aan directie en aan B&W. Het verslag bij de jaarrekening bevat in de paragraaf over bedrijfsvoering een passage over informatiebeveiliging en privacy. Dit document wordt via de website <http://pcportal.nijmegen.nl/> gepubliceerd. De rapportage die voor u ligt is een verdieping en verbreding op de passage in het jaarverslag.

Doel en scope

Gemeenten hebben in de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' van november 2013 onder meer afgesproken dat in het jaarverslag een aparte paragraaf over informatiebeveiliging wordt opgenomen. Periodieke rapportage aan alle managementlagen is onderdeel van de Baseline Informatiebeveiliging Overheid (BIO). Met deze paragraaf verantwoordt het college van B&W zich aan de gemeenteraad over informatiebeveiliging in brede zin. De separate jaarrapportage die hier voor ligt bevat de ontwikkelingen, activiteiten, incidenten en risico's met betrekking tot de onderwerpen informatieveiligheid en privacy bij de gemeente Nijmegen over het jaar 2019. Het geeft de ruimte om een beeld te schetsen van de ontwikkeldoelen voor de komende periode en de bedreigingen die van invloed zijn of kunnen zijn op de gemeente. De rapportage is in overeenstemming met het door het college vastgestelde informatiebeveiligingsbeleid. Privacy is een integraal onderdeel van dit rapport vanwege de onderlinge afhankelijkheid en samenhangende ontwikkeling.

Beleid en verantwoording

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.

De gemeente Nijmegen wil haar volwassenheidsniveau van de informatiebeveiliging verhogen. Zij streeft er naar om "in control" te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen via de Rapportage Informatiebeveiliging. In control betekent in dit verband dat de gemeente weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging. Zij weet welke (passende) maatregelen er genomen zijn en dat er een controleerbare planning is van de maatregelen die nog niet genomen zijn, die bewaakt moeten worden. Zij weet ook in hoeverre de maatregelen effectief zijn en welk risico er over blijft. Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is.

Uitgangspunten van de professionele gemeente Nijmegen

- Het informatiebeveiligingsbeleid van de gemeente Nijmegen is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving (AVG).
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en vanaf 2020 op de BIO.
- Het beleid sluit aan op het Privacy Beleid van de gemeente Nijmegen
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College van B&W van de gemeente Nijmegen. Het College van B&W herijkt periodiek het Informatiebeveiligingsbeleid.
- De werking van het Informatiebeveiligingsbeleid wordt getoetst.
- Het College van B&W van de gemeente Nijmegen is volgens de Algemene Verordening Gegevensbescherming de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. Het college ziet hier op toe.

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 dat in afstemming met het informatiebeveiligingsbeleid in 2018 is vastgesteld, wordt indien nodig herzien. 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

Algemeen Beeld en Resultaten

Huidige Stand

In 2018 schreven wij dat er veel aandacht ging naar de implementatie van de AVG op organisatieniveau, het inrichten van de rol van de Functionaris Gegevensbescherming, de Privacy Officer en de Werkgroep Privacy.

Eigenaarschap

In februari 2019 is eigenaarschap op I-bewustzijn belegd bij de afdelingen. Hierdoor is het afdelingshoofd verantwoordelijk - op organisatieniveau- voor de verwerking van persoonsgegevens binnen de betreffende afdeling. Geconstateerd kan worden dat hierdoor op afdelingen bewustwording op de AVG in relatie tot het privacy beleid toeneemt. Afdelingen zijn gestart met het opstellen van een plan van aanpak op I-bewustzijn en worden hierdoor ook gedwongen om kritisch te kijken naar de huidige werkprocessen. Bovendien hebben zij aangegeven welke BBN classificatie van toepassing is op hun gegevensverzamelingen. Verder zijn er stappen gezet op het punt van:

- Voor het SUWI stelsel: de controle werkzaamheden ten behoeve van de verantwoording.
- Aanpassingen in de werkwijze van de iRvN ten behoeve van het efficiënter verantwoorden.
- Invulling van de rollen van FG en CISO, ook na het vertrek van de Stadscontroller.

Privacy ambassadeurs

Binnen elke afdeling is naast het benoemen van eigenaarschap ook een privacy ambassadeur aangewezen. Dit is een medewerker binnen de afdeling die inhoudelijk op de hoogte is van de werkprocessen maar ook affiniteit heeft met de aspecten van de privacywetgeving. De privacy ambassadeurs hebben in het afgelopen jaar stilgestaan bij de invulling van hun rol en de eisen die dit stelt aan hun kennis en vaardigheden.

Partners

Met de invoering van de AVG is ook gekeken naar de rol en verantwoordelijkheden van onze partners. Het veilig en rechtmatig verwerken van persoonsgegevens door onze partners straalt namelijk ook uit op ons. Gelet hierop hebben wij bij alle partners de rollen en posities in het kader van de AVG vastgesteld. Samen met de partners zijn samenwerking- en verwerkersovereenkomsten gesloten en zijn gegevensuitwisselingen waar mogelijk geanalyseerd. Tevens is gemeente breed gestart met een inhaalslag op het afsluiten of actualiseren van verwerkersovereenkomsten. Verwerkers die onder verantwoordelijkheid van de gemeente Nijmegen gegevens verwerken gaan wij, afhankelijk van de inschatting van het risico dat de gegevens lopen, waar nodig intensiever beoordelen op hun verantwoordingsplicht vanuit de AVG.

Privacy by design

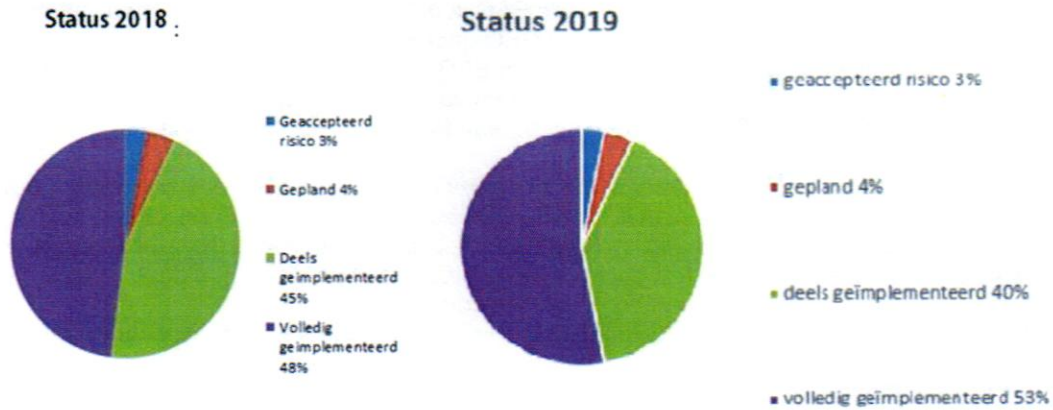
Het afgelopen jaar is kritisch gekeken naar de borging en uitwerking van Privacy by design. In samenspraak met de Radboud Universiteit zijn acht strategieën opgesteld waar nieuwe gegevensverwerkingen aan moeten voldoen. Deze strategieën zijn omgezet naar concrete eisen en wensen en zijn ingebed in het inkoopproces en bij de afdeling I&A. De praktijk blijkt weerbarstig; leveranciers vinden het lastig om in technisch opzicht aan de uitgangspunten te kunnen (of willen) voldoen. Wel zien wij een verbetering van het bewustzijn op dit onderwerp.

Control

Er is veel energie uitgegaan naar de inrichting van Stadscontrol als manier om de volwassenheid van de organisatie te vergroten. Stadscontrol is een aantal projecten gestart waarbij processen onderzocht worden op betrouwbaarheid, efficiëntie, doelmatigheid en het vermogen om te verbeteren.

ENSIA Cyclus

In 2017 is de eerste ENSIA cyclus afgerond. Om de audit last voor de gemeenten te verlichten is vanuit het Ministerie van Binnenlandse Zaken het project ENSIA (Eenduidige Normatiek Single Information Audit) gestart. Hierbij is in 2017 een integrale omgeving beschikbaar gesteld aan gemeenten waarin zij een gemeente brede zelfevaluatie op het vlak van informatiebeveiliging kunnen uitvoeren. Deze zelfevaluatie is in 2019 nog gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Vanaf 2020 zal deze gebaseerd zijn op de BIO. Of we voldoen aan deze Baseline is getoetst door middel van de zelfevaluatie die is uitgevoerd in Q3 en Q4 2019. Om de zelfevaluatie goed uit te kunnen voeren wordt de status van de BIG maatregelen bijgehouden in een management systeem (ISMS). In de loop van 2020 zal deze overgezet worden naar BIO maatregelen. Door middel van de herziening van de dataclassificatie, samen met de afdelingshoofden, zijn wij hier op voorbereid. Uit het ISMS komt de aanvullende informatie voor deze rapportage voort, zoals de samengevatte status van de maatregelen in de taartdiagrammen hier onder.



Aan de taartdiagrammen is te zien dat er net als het voorgaande jaar een kleine vooruitgang geboekt is bij het implementeren van maatregelen. Dit betreft met name maatregelen op het vlak van eigenaarschap en verantwoording. Verdere ontwikkelingen op het vlak van professionalisering worden doorgevoerd. Nu de implementatie van GGI Veilig dichterbij komt worden er stappen op het vlak van monitoring, analyse en rapportage voorbereid. Vanuit de samenwerking binnen Stadscontrol wordt er gezocht naar mogelijkheden om interne processen en externe relaties te toetsen op het veilig omgaan met informatie. Dit heeft in 2019 geleid tot het maken van een afspraak met de ODRN voor het uitvoeren van een collegiale toets, en het delen van audit informatie met de archiefinspecteur. In 2020 zal de samenwerking op het vlak van collegiale toetsing worden uitgebreid voor meerdere processen.

Wij rapporteren als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid via ENSIA. Van de horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij de rijksoverheid afgeleid, de zogenaamde verticale verantwoording. Zo zijn de informatieveiligheidsvragen over de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN) per 31 december automatisch ingevoegd bij de kwaliteitsmonitor voor verantwoording aan RvIG. Voor de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootchalige Topografie (BGT) en de Basisregistratie Ondergrond (BRO) verantwoording worden de antwoorden in ENSIA automatisch naar het Ministerie van I&W opgeleverd. De onderliggende verantwoording voor BAG, BGT en BRO is bijgevoegd in een bijlage bij deze rapportage. Een samenvatting van deze rapporten bevindt zich in de tekst hier onder.

De verantwoording over DigiD en SUWI is bijgevoegd bij de Collegeverklaring over deze twee stelsels. Voor het jaar 2019 geldt dat Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie en deze wordt getoetst door IT auditor 2Control. Met de vastgestelde Collegeverklaring (inclusief de bijlagen over DigiD en Suwinet) en het Assurancerapport voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.

BAG algemeen

Het ministerie van Binnenlandse Zaken is gestart met *Doorontwikkeling in Samenhang* van de geo-basisregistraties (DiS Geo) waarbij wordt gestreefd naar de ontwikkeling van een samenhangende objectenregistratie in 2025. We anticiperen op deze ontwikkeling bij het opstellen en doorvoeren van kwaliteitsverbeteringen voor de registraties BAG, BGT en WOZ (Waardering Onroerende Zaken).

Daarnaast heeft het verplicht gebruik van de BAG in de WOZ in 2019 geleid tot een intensievere samenwerking tussen het bureau Basis- en GEO-informatie (BAG en BGT) en bureau Gemeentebelastingen (WOZ): Koppelingen aan BAG-objecten in de WOZ zijn aangebracht en worden continue bijgehouden. Door medewerkers van Gemeentebelastingen worden terugmeldingen op de BAG gedaan aan het bureau Basis- en GEO-informatie.

In 2019 hebben we een relatie gelegd tussen de BAG en de BRP. Er is een werkwijze ingevoerd waarbij panden en verblijfsobjecten in de BAG gereed gemeld worden wanneer een burger zich inschrijft in de BRP (of een bedrijf zich inschrijft in het Handelsregister, HR). Hierdoor zijn gegevens in de BAG actueler. Het bureau Gemeentebelastingen hoeft met deze nieuwe werkwijze minder objecten te controleren op de voortgang van de bouw. Wanneer een burger zich in de BRP laat inschrijven op een adres zonder 'woonfunctie' in de BAG, is het voor de afnemers van de BAG relevant of het gebruiksdoel 'woonfunctie' in de BAG kan worden toegevoegd. De toevoeging vereist een toets op het bestemmingsplan/bouwbesluit. In 2020 wordt dit onderwerp op het niveau van het gemeentelijk managementteam besproken om te beoordelen waar keuzes gemaakt kunnen worden en of een grotere capaciteit voor het uitvoeren van deze toets geregeld moet worden.

Het mandaat voor de BAG ligt bij bureau Basis- en GEO-informatie en richt zich op uitvoering van de BAG-registratietaken. Er is in Nijmegen nog onvoldoende de relatie gelegd tussen uitvoering van de wet BAG en beleidsprogramma's. Het beleid voor Vergunningverlening, Toezicht en Handhaving (VTH) is van invloed op de volledigheid en juistheid van de registraties.

Per 1-1-2022 stelt de Waarderingskamer dat woningen gewaardeerd moeten worden op basis van 'de gebruiksoppervlakte uit de BAG'. Voor ongeveer 81.000 bestaande woningen moet hiervoor per WOZ-deelobject een berekening gemaakt worden. Door de inzet van een medewerkster via een resultaatopdracht is in 2018 en 2019 ongeveer 84% van alle uitbouw, aanbouw en opbouw van bestaande panden zonder vergunning geregistreerd. Dit gebeurt aan de hand van een constatering op de luchtfoto. In 2020 worden de resterende wijzigingen zonder vergunning geregistreerd.

Voor de juiste registraties is een uitgebreidere vraag om BAG-inspecties aan de Omgevingsdienst Regio Nijmegen (ODRN) en eventueel Handhaving volgens de WABO (Bestemmingsplan/Bouwbesluit) noodzakelijk. De beschikbare capaciteit van bouwinspecteurs van de ODRN kan door het risico-gestuurd VTH-beleid van de gemeente Nijmegen conflicteren met de behoefte voor de BAG-registratie.

Ook voor geconstateerde wijzigingen in BAG-objecten (via fotomateriaal en 3D-mutatiedetectie of terugmeldingen) geeft de wet aan om te toetsen op: 'is de wijziging vergunningsvrij of illegaal'? Deze toets gebeurt momenteel niet. In 2020 wordt dit onderwerp op het niveau van het gemeentelijk managementteam besproken om te beoordelen waar keuzes gemaakt kunnen worden en of een grotere capaciteit voor toezicht en handhaving geregeld moet worden.

BGT algemeen

In 2019 is vooral gewerkt aan het verder op orde brengen van de kwaliteit van de BGT. Het Kwaliteitsdashboard BGT van het Kadaster had 8 mijlpalen, waarvan we er 1 niet hebben gehaald. Dit is de "Uniformering van de aansluitende objecten tussen de verschillende bronhouders". In 2020 zal deze onderlinge aansluiting zal in 2020 worden afgerond. Naast de reguliere mutatie verwerking is de niet-vergunningsplichtige en illegale bebouwing met behulp van luchtfoto's van 2019 voor 84% ingemeten en verwerkt in de BGT en BAG. Daarnaast is de kruinlijn topografie aangebracht in de BGT.

In voorbereiding op de in gebruik name van het horizontale berichtenverkeer BGT-BOR (Beheer Openbare Ruimte) is in 2019 nauw samen gewerkt met BOR op het vlak van synchronisatie van de BGT met de BOR. Hiervoor heeft de BOR steeds de meest actuele BGT data ontvangen voor de koppeling met de administratieve gegevens van het groen- en wegbeheersysteem.

In 2019 is een start gemaakt met het vastleggen van het totaal proces BGT-BAG-WOZ. Een belangrijke verbetering is de inwinning van geometrie en overige informatie rond panden. In plaats van dat vanuit verschillende disciplines een pand meerdere keren wordt bezocht willen we dit zoveel mogelijk terugbrengen naar één bezoek vanuit een integrale actie. Er is ook gestart met het actualiseren van de plus-topografie in de BGT.

Met behulp van automatische mutatie detectie zullen de verschillen in topografie in beeld worden gebracht tussen de luchtfoto's van 2020 en 2019. Op deze manier krijgen we onder andere ook de laatste niet-vergunningsplichtige en illegale bebouwing in beeld.

In 2020 geven we extra aandacht aan de terugmeldingen. Doel is om deze na binnenkomst zo spoedig mogelijk af te handelen. De wettelijke termijn hiervoor is een half jaar.

BRO algemeen

De gemeente Nijmegen is stapsgewijs op weg om aan de eisen van de BRO te voldoen. De regierol ligt bij het bureau Basis- en GEO-Informatie (BRO coördinator). Samen met de inhoudelijke afdelingen werkt dit bureau aan de implementatie van de BRO.

De BRO wordt in fasen opgeleverd. In fase 1 is gewerkt aan het bewust maken van interne opdrachtgevers. Het bewustzijn is gegroeid, maar nog niet bij iedereen aanwezig. Fase 1 is in 2018 gestart en . In deze fase zijn twee van de registratieobjecten geregistreerd.

Er is in deze fase ervaring opgedaan met het afstemmen over gegevensleveringen met gegevensleveranciers, en met het controleren en leveren van gegevens via het bronhouderportaal door stadsrealisatie en vastgoed. Per volgende fase zullen de stappen opnieuw doorlopen moeten worden voor de nieuwe Registratie Objecten. Het gaat dan met name over het achterhalen en bewust maken van nieuwe interne opdrachtgevers en het implementeren van aanvullende processtappen.

Verder onderzoek blijft nodig naar aan de BRO gerelateerde processen, afdelingen en bureaus. Op basis van de door de VNG aangeleverde impactanalyse (incl. de inventarisatie van gerelateerde processen) wordt in 2020 samen met de betrokkenen verder gezocht naar een efficiënte invulling van een zo uniform mogelijk proces. Er is (en zal worden) gesproken met o.a. bureauhoofden, coördinatoren, planners, projectmanagers en -leiders, contractmanagers en adviseurs. Voor fase 2 zijn drie nieuwe registratie objecten gepland.

Resultaat Informatiebeveiliging

Waar de voorgaande paragraaf een algemeen beeld geeft zoomt deze paragraaf meer in op de details en de verdeling van de verantwoordelijkheid.

Een overzicht van de belangrijkste maatregel categorieën die bijdragen aan het realiseren van de IB doelstellingen:

1. Cruciaal bij het implementeren van informatiebeveiliging is het beleggen van de verantwoordelijkheden voor de informatiesystemen bij de juiste eigenaren. Daarnaast is ook het hebben van een informatiebeveiligingsbeleid dat geactualiseerd wordt cruciaal, zodat de door de verantwoordelijken gemaakte keuzes effectief zijn in de huidige context.
2. Waar gemeenten samenwerken, bijvoorbeeld in verbonden partijen, moet duidelijk worden vastgelegd waar welke verantwoordelijkheid ligt. De risico's die ontstaan door het delen van omgevingen en informatie moeten worden beoordeeld en ondervangen.
3. Organisatorische maatregelen omvatten het beoordelen van overeenkomsten, het hebben van een goedkeuringsproces voor ICT-voorzieningen, het hanteren van geheimhoudingsovereenkomsten en het beoordelen van dienstverlening.
4. Het classificeren van informatie op het gebruik van persoonsgegevens en het definiëren van geaccepteerd gebruik en benodigde maatregelen per classificatie.

5. Voor werknemers is het zaak te weten wat hun verantwoordelijkheden zijn. Ze dienen opgeleid te zijn om aan hun verantwoordelijkheden te kunnen voldoen. Het moet duidelijk zijn wat er verwacht wordt en wat er gebeurt als het mis gaat. Er moet scholing beschikbaar gesteld worden en documentatie.
6. Gebouwen, apparatuur en het netwerk moeten worden beveiligd tegen onbevoegd gebruik. Sleutels worden beheerd.
7. Aanpassingen aan systemen gebeuren gestructureerd en worden door de juiste rollen getest. Maatregelen tegen aanvallen worden gestructureerd genomen. Faciliteiten voor ontwikkeling, test- en productieomgevingen zijn gescheiden.
8. Toegang tot applicaties en informatie wordt beperkt tot geautoriseerde personen. Het correcte niveau van toegang wordt afgedwongen. Netwerken zijn gescheiden en verkeer en gebruik wordt gemonitord.
9. De gegevens die in applicaties ingevoerd worden, net als de uitvoer, gecontroleerd op correctheid.
10. Transport van gegevens is versleuteld. Opslag is ook versleuteld waar nodig.
11. Er wordt met grote regelmaat gezocht op kwetsbaarheden en deze worden zo snel mogelijk opgelost.
12. Er wordt gerapporteerd over de status van de informatiebeveiliging aan de CISO, de directie en aan het college. Maar ook richting de eigen organisatie (de lijn) en aan de rijksoverheid.
13. Het hebben van plannen die de continuïteit van informatiesystemen borgen. Het testen van de gemaakte plannen.
14. Weten welke wetgeving van toepassing is en de naleving daarvan kunnen aantonen aan auditors.

In het afgelopen jaar is veel aandacht uitgegaan naar punt 1, 4 en 6. Dit is de basis voor verdere ontwikkelingen in 2020 op het vlak van punt 5, 7 en 12. Bewustzijn van informatiebeveiliging is een punt waar continue aan gewerkt moet worden en continue verantwoorden, ook vanuit leveranciers, is ook iets dat in het komende jaar ingebed moet worden. Gemeente Nijmegen en de iRvN hebben in de afgelopen jaren deelgenomen aan het GGI Veilig traject. Hierdoor hebben wij nu een positie in de kopgroep en staan wij in de startblokken om het SIEM te implementeren. Hiervoor zijn voorbereidende werkzaamheden in gang gezet. Dit overzicht maakt zichtbaar hoe breed het gebied is dat de informatiebeveiliging bestrijkt.

Resultaat Privacy

Op het vlak van het treffen van maatregelen om de bescherming van de persoonsgegevens van burgers en medewerkers te waarborgen, en daarmee aan de privacy wetgeving te voldoen, zijn een aantal maatregelen getroffen. Met het vertrek van de Stadscontroller/FG heeft de Privacy Officer (PO) tijdelijk de taken van FG overgenomen. In 2020 zal onderzocht worden of de positionering van de FG logisch en functioneel is. Een besluit hierover zal moeten bijdragen aan het verder professionaliseren van de rol van de FG.

Het bijhouden van het verwerkingen register en het beoordelen van DPIA's behoren op dit moment tot de kerntaken van de PO. Op dit moment zijn er van 127 verwerkingen 119 bijpassende overeenkomsten beschikbaar. Het is bemoedigend dat het aantal registraties met geldige overeenkomsten stijgt. Omdat inkopen decentraal gebeurt vraagt het een hoge mate van bewustzijn om elke verwerking in het systeem opgenomen te krijgen. Het verwerkingenregister wordt het kader van Open en Weerbaar gepubliceerd. Het publiceren van het register van verwerkingen is geen wettelijke verplichting.

Verwerkingen



Figuur 1 De situatie in 2019

Burgers kunnen in het kader van de AVG een aantal rechten uitoefenen, zoals het recht op inzage in welke gegevens de gemeente van hen verwerkt. In 2019 zijn er 36 verzoeken ingediend bij de gemeente. Deze zijn allemaal binnen de termijn afgehandeld.

Daarnaast worden de datalekken geregistreerd. Over 2019 zijn er zo'n 48 mogelijke data gerelateerde incidenten gemeld. De toename is te wijten aan het toenemende bewustzijn bij de medewerkers van de gemeente maar ook van de iRvN. Zeven incidenten zijn gemeld bij de AP. Dit getal is vrij stabiel ten opzichte van vorige jaren. Dit zijn de gevallen die feitelijk een datalek met groot risico blijken te zijn. De resterende 41 situaties zijn beveiligingsincidenten, variërend van verloren telefoons/laptop (17), inloggen onder het account van iemand anders (3), tot situaties waarbij data door de verkeerde afdeling is ingezien, en situaties waarin de gemeente niet de verantwoordelijke is.

Jaar	Beveiligingsincidenten	Gemeld bij AP
2016	28	3
2017	34	6
2018	40	7
2019	48	7

Opvallende zaken waren het gebruik van Bittorrent; wat leidde tot een uitgebreid intern onderzoek naar download software. Daarnaast was er een klacht over gebruik van WMO informatie door een taxi chauffeur; wat leidde tot een serie gesprekken met onder andere de regionale taxi organisatie over het opslaan en uitwisselen van informatie over cliënten. Ook was er een incident met de aansturing van verkeerslichten, wat tot een reorganisatie van de toegang tot de verkeerslichten systemen heeft geleid.

De zichtbaarheid van het kenniscluster Privacy en Informatiebeveiliging, de CISO en de FG nemen nog steeds toe. Dit komt doordat de CISO en de FG meer vragen bij de afdelingshoofden hebben neergelegd en op verzoek advies geven aan hen. Besluiten worden genomen door het GMT. Daarnaast is er geïnvesteerd in de Privacy Ambassadeurs, die ook de weg naar het kenniscluster weten te vinden.

Vanuit de dataclassificatie worden maatregelen genomen om de applicaties met gevoelige gegevens beter te beschermen. Dit begint met het uitvoeren van DPIA's op deze verwerkingen. In 2019 zijn 14 DPIA's uitgevoerd. Het betreft met name nieuwe verwerkingen of bestaande verwerkingen met een hoog risico voor de betrokkene. Voor een aantal applicaties zijn

aanpassingen uitgevoerd naar aanleiding van of een DPIA, een klacht of er loopt een onderzoek naar de haalbaarheid van aanpassingen. Zo zijn bijvoorbeeld voor Excellence een aantal instellingen aangepast en is er een nieuwe werkinstructie gemaakt. De dataclassificatie wordt herzien voor het gebruik met de BIO. Ook hierbij zijn de proceseigenaren (vaak ook afdelingshoofden) nadrukkelijk betrokken. In 2019 is ook voor de herinrichting van Corsa een project gestart.

Samenwerkingen

Maatregelen belegd bij de iRvN

Van de 133 beheersmaatregelen die onderdeel zijn van de BIG zijn de onderstaande 44 maatregelen toegekend aan de iRvN. Zoals boven aangegeven vallen deze in met name technische gebieden, zoals netwerkbeveiliging, versleuteling en systeem toegang en logging. Deze maatregelen worden voor de bij de iRvN aangesloten gemeenten, de ODRN en de WBRN, op eenzelfde manier ingevuld. Van deze maatregelen gelden er 30 als volledig geïmplementeerd. Hieronder het overzicht van de maatregelen die bij de iRvN belegd zijn. In 2019 is GGI Veilig gegund. Verdere maatregelen op het vlak van bijvoorbeeld SIEM en MDM zullen in 2020 worden gerealiseerd. In 2019 is de conversie van het BIG normenkader naar BIO gestart. Gemeente Nijmegen heeft samen met de iRvN deze conversie voorbereid. De gemeente blijft eindverantwoordelijke en legt in die hoedanigheid ook over de bij de iRvN belegde maatregelen verantwoording af via ENSIA. In 2019 zal hierbij voor het eerst ervaring opgedaan worden met het verantwoorden over werking.

Code	Maatregel	Code	Maatregel
6.1.4	Goedkeuringsproces voor ICT-voorzieningen	11.4.3	Identificatie van (netwerk)apparatuur
9.1.4	Bescherming tegen bedreigingen van buitenaf	11.4.4	Bescherming op afstand van poorten voor diagnose en configuraties
9.2.2	Nutsvoorzieningen	11.4.5	Scheiding van netwerken
9.2.3	Beveiliging van kabels	11.4.7	Beheersmaatregelen voor netwerkrouting
9.2.4	Onderhoud van apparatuur	11.5.1	Beveiligde inlogprocedures
9.2.6	Veilig verwijderen of hergebruiken van apparatuur	11.5.3	Systemen voor wachtwoordenbeheer
10.1.2	Wijzigingsbeheer	11.5.4	Gebruik van systeemhulpmiddelen
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	11.5.5	Time-out van sessies
10.3.1	Capaciteitsbeheer	11.5.6	Beperking van verbindingstijd
10.4.1	Maatregelen tegen virussen	11.6.1	Beperken van toegang tot informatie

10.4.2	Maatregelen tegen mobile code	11.6.2	Isoleren van gevoelige systemen
10.5.1	Reserve kopieën maken (back-ups)	11.7.1	Draagbare computers en communicatievoorzieningen
10.6.1	Maatregelen voor netwerken	12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen
10.6.2	Beveiliging van netwerkdiensten	12.3.2	Sleutelbeheer
10.7.2	Verwijdering van media	12.4.1	Beheersing van operationele programmatuur
10.7.3	Procedures voor de behandeling van informatie	12.4.3	Toegangsbeheersing voor broncode van programmatuur
10.7.4	Beveiliging van systeemdocumentatie	12.5.1	Procedures voor wijzigingsbeheer
10.10.1	Aanmaken audit-logbestanden	12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
10.10.2	Controle van systeemgebruik	12.5.3	Restricties op wijzigingen in programmatuur
10.10.3	Bescherming van informatie in logbestanden	12.6.1	Beheersing van technische kwetsbaarheden
10.10.6	Synchronisatie van systeemklokken	15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen
11.4.2	Authenticatie van gebruikers bij externe verbindingen	15.2.2	Controle op technische naleving

Andere Samenwerkingen

In het kader van het gastheerschap vult de gemeente Nijmegen voor de MGR en de 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.

6.2.1 en 6.2.3	Omgaan met derden
7.1.2 en 7.1.3	Eigenaarschap van bedrijfsmiddelen
7.21. en 7.2.2	Verwerking van informatie
8.1.1 en 8.2.2	Verantwoordelijkheden en bewustwording
8.3.1, 8.3.2 en 8.3.3	Beëindiging dienstverband
9.1.1 – 9.1.6	Fysieke toegang
10.1.1	Documentatie van procedures
10.2.2 en 10.2.3	Toetsing van derden
10.3.2	Systeemacceptatie
10.7.1. en 10.7.4	Verwijderbare media en systeemdocumentatie
10.8.1 -10.8.5	Informatie uitwisseling
10.9.2 en 10.9.3	Online transacties
10.10.1 – 10.10.6	Logbestanden

11.1.1	Toegangsbeleid
11.2.1, 11.2.2. en 11.2.4,	
11.3.1 en 11.3.2	Wachtwoorden en gebruikersapparatuur
11.4.1, 11.4.2 en 11.4.6	Netwerkverbindingen
11.5.2	Identificatie en authenticatie
11.7.2	Telewerken
12.1.1	Analyse en specificatie
12.2.1, 12.2.2 en 12.2.3	Interne gegevensverwerking
12.4.2	Test data
12.5.4 en 12.5.5	Datalekken en software ontwikkeling
13.2.3	Bewijsmateriaal
14.1.1 – 14.1.5	Bedrijfscontinuïteit
15.1.2, 15.1.3 en 15.1.5	Bescherming van intellectueel eigendom en voorkomen van misbruik
15.3.1 en 15.3.2	Beheer van audits

De ODRN en de MGR blijven verantwoordelijk en kunnen gemeente Nijmegen bevragen op de voortgang van de implementatie van maatregelen. Hiervoor is nog geen proces afgesproken. Midden 2018 heeft de WBRN de beschikking gekregen over haar eigen Suwinet aansluiting. De auditor 2Control geeft voor de regio gemeenten die deelnemen aan de WBRN een verklaring af over het gebruik van de Suwinet aansluiting volgens de geldende normen.

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 auditor 2Control 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. Stadscontrol is bezig met het ontwikkelen van een standaard toetsingsproces.

Doelstelling gemeente Nijmegen

Realisatie

De doelstelling van de gemeente is het verhogen van haar volwassenheidsniveau van de informatiebeveiliging. Dit betekent "in control" zijn en daarover op professionele wijze minimaal jaarlijks verantwoording af te leggen via de voorliggende rapportage. In control betekent ook, in dit verband, dat de gemeente weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging. Zij weet welke (passende) maatregelen er genomen zijn en dat er een controleerbare planning is van de maatregelen die nog niet genomen zijn, die bewaakt moeten worden. Zij weet ook in hoeverre de maatregelen effectief zijn en welk risico er over blijft. Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is. Voor het "in control" zijn zou een niveau drie in CMM voldoende zijn voor een gemeente. Kijkend naar bijvoorbeeld de accountants rapportage zou de gemeente op 1 a 2 zitten.

Het voeren van minimaal de wettelijk vereiste registers (datalekken en verwerkingen) maar ook registers die nodig zijn om de omgeving te beheren en verantwoording af te leggen is onderdeel van de basis voor een gecontroleerde omgeving. Het melden (en registreren) van datalekken is een onderdeel van elke iBewustzijn workshop sinds 2017.

Om de schaarse middelen efficiënt in te kunnen zetten moeten er risico inschattingen gemaakt worden. Ook hier voor is bewustzijn nodig van de waarde van de gegevens en het beschermen er van. De dataclassificatie die in 2017 is afgerond is in 2019 herzien voor BBN, in samenwerking met de proceseigenaren wat het bewustzijn vergroot. De unit Stadscontrol ziet toe op het opvolgen van bevindingen en het nemen van de juiste maatregelen. Dit gebeurt door het voeren

van advies gesprekken en het toetsen van maatregelen. Dit laatste is iets dat in 2019 gang is gezet en in 2020 verder ontwikkeld wordt. Hiermee is een eerste begin gemaakt met het verhogen van het volwassenheidsniveau van de gemeente. Het doorvoeren van de beschreven registraties en classificatie zijn onderdeel van de voor niveau 2 gevraagde standaardisatie. Zij vormen de basis voor de risico afweging die gemaakt wordt.

Ook het iRvN en de WBRN werken aan professionalisering. Zij hebben verzoeken ingediend om in 2020 een aantal processen door gemeente Nijmegen te laten toetsen. Hiermee geven zij gehoor aan de wens van gemeente Nijmegen tot meer transparantie en verantwoording.

Evaluatie

In 2018 is vastgesteld dat het Privacy Beleid geëvalueerd zal worden. Ook het Informatiebeveiligingsbeleid is tot nu toe jaarlijks herzien, maar de invulling hier van is nog niet geëvalueerd. In 2020 zal er een evaluatie plaats vinden en zal er begonnen worden met het ontwikkelen van KPI's zoals die in het beleid worden aangekondigd. Het is de intentie dat deze evaluatie een eerste stap zal zijn in de richting van het werken met KPI's en het structureel inbedden van evaluaties van beleid. De set aan KPI's zal worden opgebouwd naarmate er meer duidelijkheid ontstaat over welke indicatoren waardevol zijn en welke niet.

De evaluatie van het privacy beleid tot nu toe geeft geen aanleiding tot een wezenlijke verandering. Er worden steeds meer DPIA's uitgevoerd die aanleiding zijn tot het maken van keuzes, bijvoorbeeld om het gebruik van gevoelige gegevens verder te beperken. Om ruimte te maken voor de evaluatie zal er voor 2020 geen wijziging van het Informatiebeveiligingsbeleid of Privacy beleid uitgebracht worden.

Perspectief

Plan voor 2020

In 2020 staan de volgende dingen gepland:

- conversie naar BIO afronden.
- Aan de slag met maatregelen die volgen uit de AVG afdelingsplannen

Voor 2020 worden in januari de plannen van de afdelingshoofden gepresenteerd met betrekking tot het AVG-proof maken van hun afdelingen. Hier uit zullen ook een aantal keuzes voortvloeien die aan het GMT van gemeente Nijmegen voorgelegd zullen worden. Denk hierbij aan de aanpak van applicaties als Corsa en het vrijmaken van capaciteit t.b.v. het doorlichten van processen. Dit zal betekenen dat de proceseigenaren mede eigenaar worden van de prioriteiten die de gemeente stelt. Stadscontrol zal deze stap monitoren en toetsen, en waar nodig begeleiden.

- implementatie van een nieuw Information Security Management System (ISMS)

De implementatie van een ISMS met meer deelnemers dan het huidige zal betekenen dat er meer kennis van eenieders rol in informatiebeveiliging in de organisatie verspreid wordt.

- maatregelen voortvloeiend uit het bezoek van de mystery guest van juni 2019
- maatregelen uit de accountantscontrole/ENSIA

Deze gemeente brede maatregelen bevinden zich op het vlak van toegang, wachtwoorden en monitoring. Aan het laatste punt zal met name de iRvN invulling geven bij de invoering van SIEM.

- maatregelen op het vlak van de kwaliteit van data (in de context van datagestuurd werken) zullen per bron worden opgepakt.
- ontwikkelen van KPI's om verantwoording te vergemakkelijken.
- opstarten interne audit trajecten bij de ODRN en de iRvN
- In 2020 zullen de Privacy Ambassadeurs meer zichtbaar worden.

De Privacy Ambassadeurs zijn gestart met het organiseren van een kennisuitwisselingsprogramma dat zij in 2020 zullen uitvoeren.

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.

Meerjarenvoorzicht Informatiebeveiliging

Toetsing

Begin 2020 wordt het Jaarplan 2020 van Stadscontrol gepresenteerd. Informatiebeveiliging en privacy vormen hier een essentieel onderdeel van. In het jaarplan wordt beschreven welke initiatieven er in 2020 zullen worden opgepakt. Het ondersteunen van en bijdragen aan initiatieven op het vlak van iBewustzijn spelen een centrale rol. In de komende jaren zullen de controle mechanismen ook toegepast worden op de toetsing van informatiebeveiligingsmaatregelen, ook bij externe relaties. Er zal intern en regionaal een "collegiaal audit circuit" opgezet worden zodat er een vinger aan de pols gehouden wordt. Door er voor te zorgen dat er een actueel beeld bestaat van hoe we er voor staan op het vlak van informatiebeveiliging wordt het gemakkelijker om verbetertrajecten op te zetten en af te ronden. Ook waar het gaat om het toe zien op de informatiebeveiliging in samenwerkingsverbanden en bij leveranciers zal het "collegiaal auditen" een belangrijk hulpmiddel zijn. 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

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 de iRvN begonnen. Op dit moment beperkt de toetsing zich tot opzet en bestaan. 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. Bewustwording blijft een onderwerp waarop veel geïnvesteerd moet worden om de benodigde cultuuromslag te bewerkstelligen. Het I-bewustzijn is bij bepaalde organisatie onderdelen hoger dan bij anderen. De cultuuromslag is ook benodigd om als organisatie meer op een lijn te komen.

Burger

In het contact met de burger blijkt dat er steeds meer verwacht wordt van de digitale mogelijkheden om diensten te verlenen en te communiceren. Zie bijvoorbeeld de ontwikkelingen rond DigiD en Eidas. Anderzijds is het zo dat er geen "one size fits all" dienstverlening 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.

Meerjarenvoorzicht 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:

Voorlichting en advies

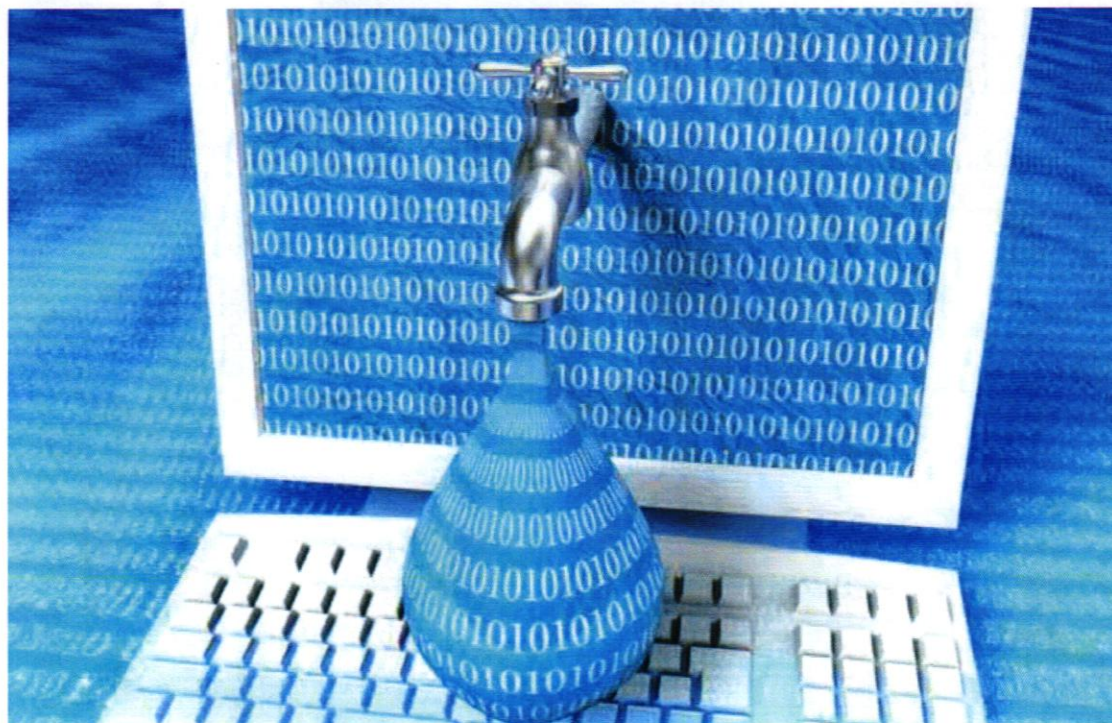
Een terugkerende vraag is hoe vanuit professie om te gaan met het gebruik van social media kanalen zoals Whatsapp, Signal of Facebook. Welke kanalen zijn geschikt om te communiceren met de burger, en welke kanalen zijn veilig voor het versturen van zakelijke informatie?

Continu proces

In het kader van risicomanagement willen wij een stevig aandachtspunt maken van de doorontwikkeling van het instrumentarium Data Privacy Impact Assessment (DPIA). Wij zijn ons ervan bewust dat het instrument DPIA op dit moment teveel een momentopname is van de privacy risico's die spelen bij een gegevensverwerking. Aan een eenmaal uitgevoerde DPIA wordt momenteel geen follow-up gegeven. Hier schuilt dan ook een kwetsbaarheid in. Tevens is het lastig om hierdoor te voldoen aan de verantwoordingsplicht. Met de afdeling Stadscontrol wordt gekeken naar de ontwikkeling van een audittraject. In de praktijk dient namelijk te blijken dat afdelingshoofden zorg dragen voor het nemen van de juiste maatregelen en dat het functioneren van de betreffende maatregelen ook door de afdeling kan worden aangetoond.

Leren van wat wij doen

Zoals bij elk thema gaan er ook wel eens dingen verkeerd. Het niet functioneren van maatregelen wordt in het ergste geval aangetoond door een datalek. Het bewust worden van de organisatie is het meest gediend als we daar een leermoment van kunnen maken. Juist door het leren van onze ervaringen ontstaat de mogelijkheid om beter te worden. Het breder uitdragen van deze geleerde lessen kan helpen in de bewustwording en daarmee weerbaarder maken van medewerkers en bestuurders. Stadscontrol heeft in 2019 onderzoek gedaan naar het organisatie principe "Leren van wat we doen". De conclusies uit dit onderzoek zullen in 2020 worden getrokken hoe op langere termijn de organisatie beter in staat is te leren.



Rapportage Informatiebeveiliging en Privacy 2020

Informatiebeveiliging & privacy

2020

Resultaten



Inzage-verzoeken burgers

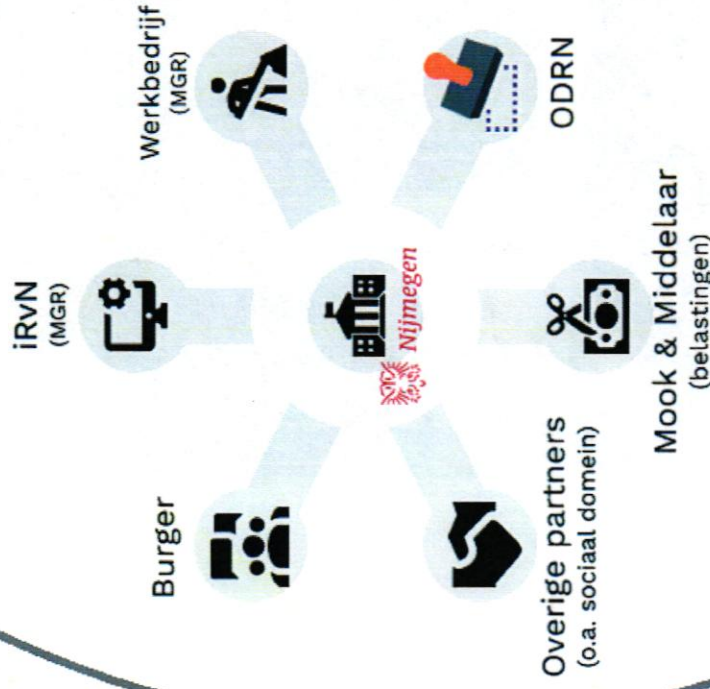


Persoonsgegevens verstrekt aan derden



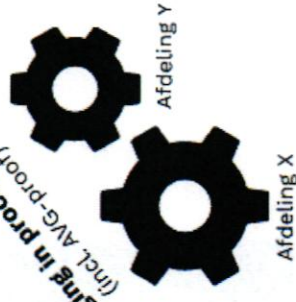
Verwerkersovereenkomst
(over verantwoord gebruik gegevens burgers/medewerkers)

Ons speelveld



Uitdagingen

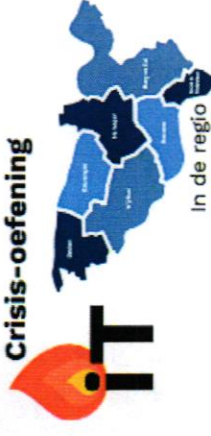
Bordring in processen
(incl. AVG-proof)



I-bewustzijn



Crisis-oefening



Inhoudsopgave

1. Doel & wettelijk kader	4
2. Leeswijzer	4
3. Ambitie	4
4. Terugblik	6
4.1 Wat wilden we bereiken?	6
4.2 Wat hebben we bereikt?	6
5. Vooruitblik	11
5.1 Aanbevelingen uit externe toetsing	11
5.2 Komend jaar	12
5.3 Meerjarig	13
Bijlage: achtergrond & begrippen	15

1. Doel & wettelijk kader

Doel

In dit rapport informeren we u over de ontwikkeling van de informatiebeveiliging bij de gemeente Nijmegen. We kijken terug op het afgelopen jaar en kijken vooruit naar de ontwikkelingen in 2021 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 de 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 kijken 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 2020 boekten en 3) de uitdagingen waar we in de toekomst voor staan.

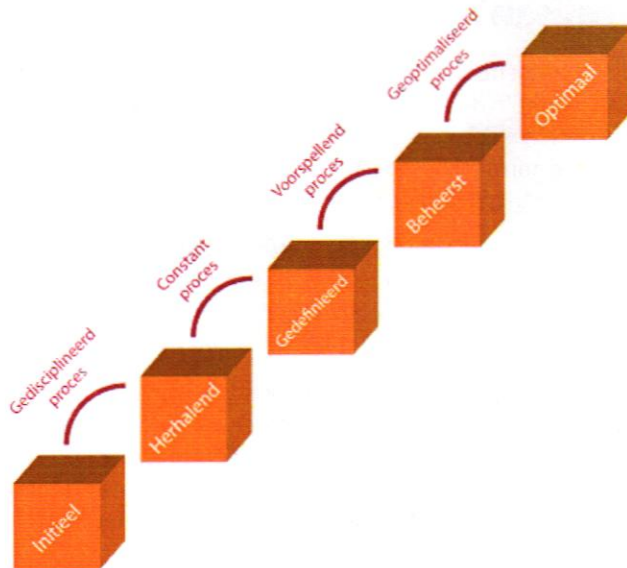
In de bijlage vindt u achtergrondinformatie over informatiebeveiliging & privacy inclusief een toelichting op veel gebruikte begrippen.

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. 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.

Ambitie

Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is.



Figuur 1 Capability Maturity Model vertaald

De mate van 'in control zijn' kan uitgedrukt worden in volwassenheidsniveaus in het CMM model¹, zoals ook de accountant doet. De gemeente streeft naar niveau 3 in dit model. Dit is het niveau waarop processen zodanig goed gedefinieerd zijn dat ze ook goed functioneren als omstandigheden veranderen (bijvoorbeeld als medewerkers van functie veranderen). De kwaliteit van het proces meten we objectief gemeten.

Met de oprichting van het team Stadscontrol binnen de gemeentelijke organisatie en het hierin onderbrengen van de CISO en de FG is de controlerende en oordeelsvormende rol binnen de gemeente meer voor het voetlicht gebracht. 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 het iRvN en de WBRN werken aan professionalisering. Zij hebben verzoeken ingediend om in 2020 een aantal processen door gemeente Nijmegen te laten toetsen. Hiermee geven zij gehoor aan de wens van gemeente Nijmegen tot meer transparantie en verantwoording ook naar hun andere partners toe.

¹ <https://www.ictloket.nl/kennisbank/mkb-marketing/marketingmodellen/capability-maturity-model-integration-cmmi/>

4. Terugblik

4.1 Wat wilden we bereiken?

In 2020 ging veel aandacht uit naar het inrichten van de CyberManager. Dit is een programma dat de gemeente ondersteunt bij het verkrijgen van inzicht in de risico's die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen. Onderdeel van de invoering van de CyberManager was de overgang naar het nieuwe normenkader BIO, waarin eigenaarschap en risicomanagement een veel grotere rol spelen dan in het vorige, meer normgerichte kader.

Daarnaast was het zoeken naar wat er mogelijk was tijdens de Corona pandemie. Afdelingen zijn gestart met het uitvoeren van het AVG-proof plan. 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 blijvend aandacht besteden aan iBewustzijn is onderdeel van de jaarlijkse plannen evenals het opvolgen van de aanbevelingen van de accountant, IT-auditor en de resultaten van andere toetsingen. De Citrix crisis bleek daarbij een goede aanleiding om de crisisorganisatie van de gemeente te evalueren. Dit heeft geleid tot nieuwe proces afspraken. Daarnaast wilden we in de regio aan de slag met collegiale toetsing en het (ethisch) laten hacken van de iRvN. Dit hebben we moeten uitstellen tot 2021.

4.2 Wat hebben we bereikt?

4.2.1 De gemeente Nijmegen

Activiteiten over de hele gemeente

- Het AVG-proof project van Zorg en Inkomen, en Publiekszaken, heeft in 2020 een goede start gemaakt onder een voortvarende projectleider. Een stuurgroep is aan de slag gegaan met de gemeentebrede implementatie van de AVG maatregelen. Hierdoor is er meer zicht op de stand van zaken en de voortgang.
- De Functionaris Gegevensbescherming zal de implementatie van de maatregelen gemeentebreed monitoren door de uitvoering van het controleplan dat hij dit jaar heeft opgesteld.
- Het in- en uitstroomproces van medewerkers is herzien.
- Bitwarden is als standaard wachtwoord manager ingevoerd.
- De CISO's hebben regionaal een phishing mail campagne uitgevoerd.
- Per 1 juli zijn de betreffende strategisch adviseurs van Stadscontrol tot Functionaris Gegevensbescherming en CISO benoemd. 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 en het toetsen van maatregelen, bijvoorbeeld door het uitvoeren van audits met behulp van de CyberManager.

Invoering van de CyberManager uitgelegd

Om compleet en actueel inzicht te hebben in hoe de gemeente er op het vlak van informatiebeveiliging, en het voldoen aan de AVG, voor staat is er een systeem nodig waarin we de status van de maatregelen die we nemen bijhouden. Een dergelijk systeem is een Information Security Management System (ISMS). Tot en met 2019 gebruikten we hier voor een product van SEP². In 2020 zijn we overgestapt op

² <https://sep.nl/isms/>

een ander product, de CyberManager³. Tijdens deze invoering hebben we de informatie die in het oude systeem zat overgezet naar het nieuwe normenkader dat in 2020 verplicht werd, de Baseline Informatiebeveiliging Overheid (BIO).

Omdat de manier waarop de systemen werken erg verschilt hebben we de overzetting van de informatie uitgevoerd door in de CyberManager een “interne audit” uit te voeren op de status van de BIO maatregelen. Hierbij hebben we samen met de leverancier handmatig alle informatie uit het SEP systeem overgenomen en ingevoerd in de CyberManager.

De CyberManager drukt de implementatiestatus uit in aparte scores voor of iets beschreven is of dat er bewezen kan worden dat iets feitelijk ook zo werkt. De SEP implementatie statussen zijn vertaald naar de CyberManager statussen. Voor de SEP status “Geaccepteerd risico” is in de CyberManager de norm “Niet van toepassing” verklaard met de toelichting “Geaccepteerd risico” gebruikt.

De resulterende situatie is dat de status en historische informatie nu beschikbaar is in de CyberManager en kan dienen als uitgangspunt voor verdere implementatie van de BIO.

In de infographic voorin kunt u zien dat in de CyberManager nu 70% van de maatregelen actief is. De voortgang bij het implementeren van de maatregelen zal van 2020 op 2021 goed meetbaar zijn via de CyberManager. Met de omzetting is een eerste begin gemaakt met het verhogen van het volwassenheidsniveau van de gemeente.

IT Audit observaties van de Accountant over 2020

De jaarlijkse accountantscontrole heeft een aantal positieve ontwikkelingen laten zien en legt ook een aantal kwetsbaarheden bloot. Deze zijn na te lezen in het IT rapport van de accountant. Positief is dat we meer grip hebben gekregen op het loggen van meldingen uit systemen, het in- en uitdienst proces en de controle op autorisaties. We kunnen betrouwbaar afwijkingen zien in processen. Dit hoort bij CMM volwassenheidsniveau 2 voor detectie (zie hoofdstuk 3). In het afgelopen jaar zijn we op het vlak van het reageren op afwijkingen (response) naar niveau drie opgeklommen. Het lukt dus om incidenten telkens goed af te handelen onafhankelijk van wie het oppakt.

De accountant is minder te spreken over het niet evalueren van het informatiebeveiligingsbeleid en monitoring door KPI's en het niet volledig betrekking van de eigenaren van Nijmegen in het wijzigingsproces. Hiervoor is een verbetertraject opgestart samen met de iRvN en met advies van de accountant. Kijkend naar de accountantsrapportage zit de gemeente voor het merendeel op niveau een en twee, het niveau waar we afhankelijk zijn van de expertise van specifieke medewerkers. Voor governance en response zitten we nu op niveau drie.

Resultaat van de ENSIA Cyclus 2020

De zelfevaluatie is in gebaseerd op de BIO. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd.

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

³ <https://www.cybermanager.nl/software/>

Stelsel	Samenvatting
DigiD	Strengere handhaving op normen betekent voor DigiD dat van de 25 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	Over het algemeen zijn de uitslagen van het jaar 2020 goed. Wij voldoen aan de wettelijke eisen. Aan de verbeterpunten uit 2019 is in 2020 gewerkt zoals bijvoorbeeld aan het punt van functiescheiding.
Reis-documenten	De uitslagen van het jaar 2020 zijn goed.
BAG	Over het jaar 2020 voldoen wij aan de norm score voor de BAG. In 2020 is de samenwerking tussen het bureau Gemeentebelastingen (WOZ) en het bureau Basis- en GEO-informatie (BGT en BAG) sterk verbeterd op het gebied van het (verplicht) gebruik van gegevens. Hiermee zijn de verschillen in de gegevens verder teruggebracht wat de actualiteit en kwaliteit verhoogt.
BGT	Over het jaar 2020 voldoen wij aan de norm score voor de BGT. In 2020 hebben we veel tijd en aandacht besteed aan verschillende projecten om daarmee de kwaliteit van de data in de basisregistraties BGT, BAG en WOZ meer gelijk te krijgen. Daarnaast hebben we de reguliere opdrachten allemaal kunnen verwerken in de BGT. Dit betekent dat we bij zijn conform de wettelijke vereisten in het verwerken van de veranderingen die in de stad zijn gedaan.
BRO	Over het jaar 2020 voldoen wij aan de norm score voor de BRO. Begin 2020 zijn er vervolgstappen gezet om de organisatie rond de BRO verder vorm te geven. Er zijn presentaties gegeven en gesprekken gevoerd met de afdelingen Stadsontwikkeling, Stadsrealisatie en -beheer. Ook is er in maart een vervolggesprek geweest met de projectleiders van bureau Vastgoed.

Resultaat op het vlak van privacy

Als het gaat om het treffen van maatregelen om de persoonsgegevens te beschermen is een aantal stappen gezet. Het bijhouden van het verwerkingen register en het uitvoeren van gegevensbeschermingseffectbeoordelingen behoren op dit moment tot de kerntaken van de tweedelijns adviseur voor privacy, de Privacy Officer. De gegevens rond de verwerkingen ziet u in de infographic. Het aantal registraties met geldige overeenkomsten stijgt. Omdat inkopen decentraal gebeurt vraagt het een hoge mate van bewustzijn om elke verwerking in het systeem opgenomen te krijgen. Het verwerkingenregister wordt in het kader van Open en Weerbaar manifest gepubliceerd. Het publiceren van het register van verwerkingen is geen wettelijke verplichting.

Burgers kunnen in het kader van de AVG een aantal rechten uitoefenen, zoals het recht op inzage in welke gegevens de gemeente van hen verwerkt. Daarnaast worden de datalekken geregistreerd. Het aantal incidenten en datalekken is terug te zien in de infographic.

Het aantal incidenten is gedaald terwijl het aantal meldingen bij de AP is gestegen. Er zijn opvallend minder telefoons verloren in het afgelopen jaar. Dit is wellicht een gevolg van de lockdowns. Daarnaast

zijn er in het afgelopen jaar meer meldingen gemaakt in het zorgdomein ten opzichte van 2019. Meldingen in het zorgdomein leiden vrijwel altijd tot een melding bij de AP. Dit verklaart het hogere aantal meldingen daar. Een aantal opvallende meldingen betreffen gesprekken rond casussen die gemeld werden in het sociaal domein. Binnen de gemeente zal bepaald moeten worden hoe om te gaan met zorgen rond collega's zonder hun privacy te schenden. Ook zijn er een aantal meldingen gedaan door Publiekszaken. Vanwege de gegevens die bij Publiekszaken verwerkt worden volgt ook hier vrijwel altijd een melding bij de AP. De meldingen bij Publiekszaken leidden daar tot een project waarin het proces herzien wordt om de kwetsbaarheid die ontstaat door het omgaan met papieren dossiers verder te beperken.

Het aantal meldingen wordt sterk beïnvloed door de meldingsbereidheid van de medewerker. Daarbij is zorg ontstaan voor mogelijke sancties voortkomend uit een melding. In het komende jaar is het belangrijk om in het kader van iBewustzijn aandacht te besteden aan het feit dat melden altijd belangrijk is en niet afgestraft zal worden met sancties, om te voorkomen dat de meldingsbereidheid af neemt.

4.2.2 iRvN

In reactie op de aanbevelingen van de accountant en gebeurtenissen als de hack van de universiteit van Maastricht is de iRvN het veiligheidsproject gestart. Dit project omvat een aantal doelen:

- een aanval voorkomen
- een aanval zo snel mogelijk ontdekken (detecteren)
- een gedetecteerde aanval inperken en zo snel mogelijk stoppen

Dit betekent dat het netwerk verder opgedeeld is in een apart netwerk voor beheerstaken en een kantoornetwerk. Er worden ook verschillende accounts gebruikt voor deze netwerken. Zo komen de accounts met beheerdersrechten niet op het kantoornetwerk wat voorkomt dat een aanvaller veel rechten krijgt. 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 aansluiting met de kopgroep op het landelijke detectiesysteem (SIEM) is ook tot stand gebracht. Daarnaast worden de laptops opnieuw ingericht met meer beperkingen op toegang zodat problemen voorkomen kunnen worden. De gemeente blijft eindverantwoordelijk en legt in die hoedanigheid ook over de bij de iRvN belegde maatregelen verantwoording af via ENSIA.

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 collegiale toetsing van de informatiebeveiligingsmaatregelen zoals verwerkers die moeten invoeren om de gemeente te ondersteunen. In 2020 is een begin gemaakt met de collegiale toetsing bij de ODRN.

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

Terugblik

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.

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. Stadscontrol is bezig met het ontwikkelen van een standaard toetsingsproces.

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 aangegeven 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.


IT toegangsrechten (PIF)
Toekenning gebruikersrechten in applicatie + periodiek beoordeling


IT


Cyber-security (PIF)
Info-beveiligingsbeleid
Aantoonbare IT-beheersing IRvN
Persoonlijke apparaten

- Op aanraden van de accountant gaan we een meerjarenplan opstellen rondom IT. Specifiek op de toegangsbeveiliging is ons streven om rechten toe te kennen op basis van rollen in plaats dit per persoon te doen. Daarbij adviseert de accountant om rechten ook periodiek te beoordelen.
- 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 de iRvN wordt aangeraden om toe te werken naar een certificering van de iRvN, door een onafhankelijke partij, over de betrouwbaarheid van hun processen. Met dit als vergezicht, is ons voornemen om als tussenstop interne audits uit te voeren met behulp van de CyberManager.
- Afsluitend willen we het ‘mobile device management’ rondom het gebruik van persoonlijke apparaten (o.a. smartphones en tablets) uitbreiden. Het formuleren van beleid (soms regionaal) maakt hier een onderdeel van uit.
- Tot slot raadt de accountant ons aan om meer gebruik te maken 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 bevestigden zij een aantal afwijkingen voor DigiD en Suwinet.

In de verklaring die het college jaarlijks af geeft over het voldoen aan de wettelijke normen voor het gebruik van DigiD en Suwinet staat voor 2020 dat wij voor een aantal normen niet voldoen. Dit betekent voor DigiD dat van de 25 normen per aansluiting bij twee van de vier aansluitingen er twee niet voldoen. Voor Suwinet betekent dit dat aan de twee toepassingen die wij al kenden er een is toegevoegd. Daarnaast is het zo dat er van de veertien normen die gelden voor de twee bekende toepassingen er een niet voldoet.

- De Suwinet toepassing die wij niet kenden wordt verzorgd door een van onze leveranciers. Het bleek dat wij niet voldoende op de hoogte waren van het gebruik van inkomensgegevens door deze leverancier, onder onze verantwoordelijkheid.
- De tweede Suwinet opmerking heeft betrekking op hoe wij de controle op het gebruik van Suwinet in onze eigen organisatie hebben geregeld met name voor nieuwe toepassingen in het Zorg domein.

Alle aanbevelingen zijn onderdeel van het verbeterplan voor het komende jaar.

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 2021 staan de volgende stappen gepland:

- Implementatie van de CyberManager afronden
- maatregelen die volgen uit de AVG afdelingsplannen
- maatregelen van de mystery guest van juni 2019
- 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 de iRvN in 2020 heeft uitgevoerd, en dat in 2021 afgerond zal worden.

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. 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 de iRvN begonnen. Op dit moment beperkt de toetsing zich formeel tot opzet en bestaan, al zal er wel een eerste proef plaats vinden op het toetsen 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 burger 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:

Voorlichting en advies zijn onontbeerlijk

Een terugkerende vraag is hoe vanuit professie om te gaan met het gebruik van social media kanalen zoals Whatsapp en Signal of Facebook, naast het gebruik van reguliere kantoor applicaties zoals (versleutelde) mail. De Citrix crisis heeft laten zien dat er bij het gebruik van social media kanalen vragen ontstaan op het vlak van archivering, wat een eis is voor zakelijk gebruik. Daarnaast ontstaat er door de Corona crisis steeds meer vraag naar applicaties die samenwerken op afstand ondersteunen, zoals bijvoorbeeld Miro. Telkens moet hier de afweging gemaakt worden tussen gebruiksgemak en de waarborgen voor het veilig omgaan met persoonsgevoelige informatie. Deze afweging maakt de organisatie zelf bij het formuleren van beleid, maar ook de medewerker maakt deze afwegingen dagelijks bij het uitvoeren van werkzaamheden de keuzes rond de te gebruiken gereedschappen en de te delen informatie.

Evaluatie als continu proces

In het kader van risicomanagement voeren wij Data Privacy Impact Assessments (DPIA) uit op nieuwe en bestaande gegevensverwerkingen. Dit zijn analyses aantonen wat de risico's van de gegevensverwerking zijn voor de privacy van de betrokkenen (meestal burgers). Deze analyses zijn op dit moment nog te vaak een momentopname van de privacy-risico's die spelen bij een gegevensverwerking. Afdelingen die een DPIA hebben uitgevoerd doen dit meestal maar een keer en gebruiken het niet als terugkerend evaluatie-instrument bij proceswijzigingen. De DPIA kan ook gebruikt worden om het invoeren van de ingezette maatregelen te monitoren en te borgen. Ook dat zien we nog niet. Door de DPIA ook in te zetten bij beheer / controle zal het nadrukkelijk een onderdeel vormen van de (interne) verantwoordingsplicht.

Leren van wat wij doen

Zoals bij elk thema gaan er ook wel eens dingen verkeerd. Het niet functioneren van maatregelen wordt in het ergste geval aangetoond door een datalek. Het bewust worden van de organisatie is het meest gediend als we daar een leermoment van kunnen maken. Juist door het leren van onze ervaringen ontstaat de mogelijkheid om beter te worden. Het breder uitdragen van deze geleerde lessen kan helpen in de bewustwording en daarmee weerbaarder maken van medewerkers en bestuurders

Dit heeft onder andere geleid tot een voorstel tot het benoemen van iBewustzijn als belangrijk thema voor de Nijmegen School vanaf 2021.

In het kader van leren van wat we doen ondersteunt Stadscontrol het iBewustzijn programma met aanvullende activiteiten op het vlak van gedrag en cultuur.

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 Grootchalige 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 is 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 Assessment 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.

