De Rekenkamer neemt een onafhankelijke positie in binnen de gemeente Nijmegen.

Nijmegen

Postadres
Gemeente Nijmegen
BM60
Postbus 9105
6500 HG Nijmegen

Bezoekadres
Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactpersoon
Jelly Smink
j.smink@nijmegen.nl
T 024 – 329 23 38

Ons kenmerk
BM60/07/E22.001177

Gemeenteraad gemeente Nijmegen

(iaa: College van B&W, fracties)

Datum 1 juli 2022
Betreft Rapport regionaal rekenkameronderzoek 'Weten wat je moet weten'

Geachte leden van de gemeenteraad,

Hierbij bieden wij u het eindrapport aan van ons onderzoek naar informatiebeveiliging en privacybescherming, dat wij samen met de rekenkamer(commissie)s van Berg en Dal, Beuningen en Wijchen hebben gedaan.

De uitkomsten van het onderzoek laten veel overeenkomsten tussen onze gemeenten zien, maar er zijn ook verschillen. Om die reden zijn er verschillende versies van het rapport opgesteld voor de vier gemeenten. U vindt de rapporten van alle gemeenten via de website van de gemeente Nijmegen: https://www.nijmegen.nl/over-de-gemeente/rekenkamer/onderzoeksrapporten/informatiebeveiliging-en-privacybescherming/

Bijgevoegd is het rapport voor de gemeente Nijmegen. Het rapport bevat naast de uitkomsten een aantal concrete aanbevelingen om de informatiebeveiliging en privacybescherming verder te verbeteren. Achteraan in het rapport vindt u de bestuurlijke reactie van het college en het DB van de MGR Rijk van Nijmegen, en het nawoord van de rekenkamer.

Wij zijn ons ervan bewust dat de aanbevelingen een forse inspanning vergen van het college van B&W. Dat neemt niet weg dat ons inziens alle aanbevelingen - in samenhang - moeten worden opgepakt. Uiteindelijk zijn het raad en college die samen moeten afspreken in welke volgorde en met welk tijdpad aan de slag wordt gegaan.

Hoe gaat het verder?
Wij willen de raad vragen om het rapport zo snel mogelijk na de zomer te agenderen. Als rekenkamer komen we het graag toelichten. Wij bieden de griffiers van de vier betrokken gemeenteraden ook aan om mee te denken over opstelling van het raadsvoorstel. Een concrete suggestie aan de raden en griffiers is om de toelichting op het rapport in regionaal verband te organiseren.

Wanneer u vragen heeft naar aanleiding van deze brief, kunt u contact met de secretaris van de Rekenkamer opnemen: j.smink@nijmegen.nl of 024 – 329 23 38.

Met vriendelijke groet,

G. Backus
Voorzitter Rekenkamer Nijmegen

J. Smink
Secretaris Rekenkamer Nijmegen

Rekenkamer(commissie)s
Berg en Dal, Beuningen, Nijmegen en Wijchen



BIJLAGENBOEK GEMEENTE NIJMEGEN

Weten wat je moet weten

Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming

Juli 2022

COLOFON

Dit bijlagenboek hoort bij het rapport dat op basis van een gezamenlijk onderzoek naar informatiebeveiliging en privacybescherming is opgesteld door de rekenkamer(commissie)s van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen. De bijlagen 1 tot en met 7 zijn voor alle gemeenten gelijk. Voor de gemeente Nijmegen is er een extra bijlage: bijlage 8. Voorliggend bijlagenboek betreft die voor Nijmegen.
Voor elk van de vier gemeenten die zijn onderzocht is een aparte versie van het rapport opgesteld. Op onderdelen verschillen die versies van elkaar, omdat er behalve veel gezamenlijke bevindingen ook verschillen zijn tussen de gemeenten. Elk rapport is te vinden op de website van de betreffende rekenkamer of bij de rekenkamer op te vragen.

Telefoon	**Website**	**E-mail**
Berg en Dal		
06 28 74 38 98	www.bergendal.nl/rekenkamer	griffie@bergendal.nl
Beuningen		
14 024	Gemeente Beuningen / Rekenkamer	
Nijmegen		
024 – 329 23 38	https://www.nijmegen.nl/over-de-gemeente/rekenkamer/onderzoeksrapporten/	rekenkamer@nijmegen.nl
Wijchen		
088 – 432 72 03	www.wijchen.nl	griffie@wijchen.nl

Bij de uitvoering van het onderzoek zijn de rekenkamer(commissie)s ondersteund door onderzoekers van:

- DMC Group (onderdeel informatiebeveiliging): drs. Chris P.J. Deben CISM, ing. Henk Struving CISA CISSP CISM Lead auditor ISO 27001 en Mick Deben BSc CISSP CRISC;
- Legal2Practice (onderdeel privacybescherming): mr. Jean Paul van Schoonhoven BBA CCO SIO FIP CIPM CIPT CIPP/E, Meindert Boon RA CDPP CIPM CIPP/e, Philippe Dauphin MA BCS Data Protection en Wilfred Brom BC;

Bij het opstellen van de rapportage zijn de rekenkamer(commissie)s ondersteund door drs. Etienne Lemmens van Prae Advies & Onderzoek.

INHOUDSOPGAVE BIJLAGENBOEK

Bijlage 1: Aanpak van het onderzoek: deelvragen en gesprekspartners

Bijlage 2: Normenkader, inclusief een toelichting op de gehanteerde volwassenheidsmodellen

Bijlage 3: 10 bestuurlijke principes informatiebeveiliging en VNG-resoluties

Bijlage 4: Overzicht van verplichte BIO-documenten

Bijlage 5: Strategische, tactische en operationele kaders uit Basisafspraken gemeenten - iRvN

Bijlage 6: Voorbeeld verantwoordingsrapportage aan de gemeenteraad

Bijlage 7: Verklaring van gebruikte begrippen en afkortingen

Bijlage 8: P&C-documenten over informatiebeveiliging en privacybescherming

De bijlagen 1 tot en met 7 zijn voor alle vier gemeenten identiek. Voor de gemeente Nijmegen is er één extra bijlage (bijlage 8: P&C-documenten over informatiebeveiliging en privacybescherming).

BIJLAGE 1: AANPAK VAN HET ONDERZOEK: DEELVRAGEN EN GESPREKSPARTNERS

In hoofdstuk 1 van het regionale rekenkamerrapport 'Weten wat je moet weten' over informatiebeveiliging en privacybescherming is een toelichting gegeven op de aanleiding, opzet en aanpak van het onderzoek. Op een aantal onderdelen is in deze bijlage meer in detail ingegaan, namelijk:

- de deelvragen die leidend geweest zijn bij het onderzoek;
- de geïnterviewde bestuurders en functionarissen;
- de deelnemers aan de expertmeeting.

Deelvragen die leidend waren bij de uitvoering van het onderzoek

De vraagstelling van het onderzoek is:

1. Is de informatiebeveiliging en privacybescherming van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen voldoende op orde, is er voldoende zicht op de risico's en werken de gemeenten op effectieve en efficiënte wijze aan verbetering van de onderdelen die niet voldoende op orde zijn?
2. Hoe kunnen de gemeenteraden de komende jaren hun kaderstellende en controlerende taak op deze thema's goed vervullen?

Om deze vragen te beantwoorden zijn deelvragen geformuleerd. We onderscheiden:

- onderzoeksdeel A voor de informatiebeveiliging;
- onderzoeksdeel B voor privacybescherming;
- onderzoeksdeel C voor de rol van de raad.

De deelvragen zijn leidend geweest bij de uitvoering van het onderzoek.

Deelvragen onderzoeksdeel A: Informatiebeveiliging

A1. Hoe zijn de taken en verantwoordelijkheden op het terrein van ICT- en informatiesystemen en met name de informatiebeveiliging tussen de gemeenten en iRvN verdeeld?

A2. Wat zijn de beleidskaders van de gemeenten en de iRvN t.a.v. hun informatiebeveiliging, met name van persoonsgegevens?

A3. Voldoen deze beleidskaders aan de gangbare standaarden en wetgeving op het vlak van privacy en informatiebeveiliging?

A4. Wat is het beschikbare budget van de deelnemende gemeenten en iRvN voor informatiebeveiliging, en is het mogelijk om een oordeel te geven (bijvoorbeeld door benchmarking) over de toereikendheid hiervan?

A5. In hoeverre worden de beleidskaders in de praktijk in de gemeenten en de iRvN nageleefd?

A6. Op welke manier worden gemeentelijke medewerkers bewust gemaakt van hun verantwoordelijkheden ten aanzien van het bewaken van de informatiebeveiliging? Daarbij kan worden gedacht aan onder meer trainingen en ondersteuning, maar ook via functieomschrijvingen, aandacht in functioneringsgesprekken etc.

A7. Heeft de gemeente een proces van continue verbeteren in werking voor haar informatiebeveiliging en opslag en beheer van persoonsgegevens in het bijzonder?

A8. Hebben de gemeenten en de iRvN voldoende zicht op de risico's (zowel veiligheidsrisico's als financiële risico's ingeval van lekken of incidenten) op het gebied van informatiebeveiliging, en zijn er maatregelen getroffen om de grootste risico's te kunnen ondervangen?

A9. Hebben de gemeenten en de iRvN een concreet plan voor het effectief en efficiënt verkleinen van de risico's, en voldoet dat plan aan de gebruikelijke standaarden?

Deelvragen onderzoeksdeel B: Privacybescherming

Onderzoeksdeel B richt zich op de omgang met persoonlijke gegevens van burgers door de gemeenten, waar relevant ook door iRvN.

Om het onderzoek uitvoerbaar te houden, hebben wij ervoor gekozen ons bij onderzoeksdeel B te focussen op het sociaal domein, in het bijzonder:

- de verwerkingen van persoonsgegevens door gemeenten in het kader van de Jeugdwet;
- het verstrekken van persoonsgegevens:
    - binnen gemeenten aan medewerkers Openbare Orde en Veiligheid
    - door gemeenten aan samenwerkingsverbanden op het gebied van openbare orde en veiligheid (zoals Veiligheidshuizen en RIECS[1]).

B1. Wat zijn de gemeentelijke beleidskaders t.a.v. privacybescherming in het sociaal domein? Hoe wordt er geanticipeerd op de AVG?

B2. Voldoen deze beleidskaders aan de gangbare standaarden en wetgeving?

B3. Hoe is het beleid uitgewerkt en geborgd in processen? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B4. Hoe is de toegang tot dossiers (autorisaties) geregeld? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

[1] RIEC: Regionaal Informatie- en Exptertise Centrum. De tien RIECs en het LIEC (landelijk Inforamtie- en Exptertisecentrum) ondersteunen partners bij de aanpak van georganiseerde criminaliteit.

B5. In hoeverre worden de beleidskaders en vastgestelde processen en regels nageleefd in de praktijk in de gemeenten (en binnen de iRvN)? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B6. Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?

B7. Op welke manier worden burgers geïnformeerd over het gebruik en de verwerking van hun persoonsgegevens?

B8. Hoe ziet het toezicht op de omgang met de persoonsgegevens eruit, op papier en in de praktijk? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B9. Op welke manier worden gemeentelijke medewerkers bewust gemaakt van hun verantwoordelijkheden ten aanzien van het bewaken van de privacy van persoonsgegevens? Daarbij kan worden gedacht aan onder meer trainingen en ondersteuning, maar ook via functie-omschrijvingen, aandacht in functioneringsgesprekken etc.

B10. In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom de bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds?

Deelvragen onderzoeksdeel C: Kaderstelling en controle door de gemeenteraden

C1. Op welke wijze verloopt het proces van kaderstelling en controle door de gemeenteraden tot op heden t.a.v. de informatiebeveiliging en privacybescherming in hun gemeente, en hoe moet dit proces en het resultaat ervan worden beoordeeld?

C2. Op welke wijze faciliteren de colleges de kaderstelling en controle door de gemeenteraden, met name ten aanzien van de informatievoorziening aan de raden?

C3. Welke voorwaarden en vereisten kunnen worden geïdentificeerd om de kaderstelling en controle beter te laten verlopen? In het bijzonder moet daarbij aandacht zijn voor de inrichting van de informatievoorziening.

C4. Zijn er elders in het land relevante best practices ten aanzien van een goed verlopend proces van kaderstelling en controle door de gemeenteraad op dit gebied, en wat zijn de belangrijkste lessen die daaruit kunnen worden geleerd?

Gesprekken met betrokkenen

In de volgende tabel is aangegeven met welke bestuurders en functionarissen[2] binnen gemeente en iRvN is gesproken en op welk(e) onderde(e)l(en) van het onderzoek de focus lag: informatiebeveiliging (A), privacybescherming (B) of de rol van de gemeenteraden (C).

Geïnterviewde bestuurders en functionarissen	**Informatie Beveiliging (A)**	**Privacy Bescherming (B)**	**Rol gemeenteraad (C)**
Gemeente Berg en Dal			
Portefeuillehouder ICT	X		
Chief Information Security Officer /ENSIA-coördinator	X		
Functioneel beheerder	X		
Functionaris Gegevensbescherming	X	X	
Gemeentesecretaris	X		
Kwaliteitsmedewerker Documentaire Informatievoorziening	X		
Kwaliteitsmedewerker Jeugd/Wmo (2)		X	
Opgavemanager	X		
Teamleider Sociaal Team en Regieteam		X	
Teamleider Team Informatie	X	X	
Vertegenwoordiger griffie			X
Gemeente Beuningen			
Burgemeester / portefeuillehouder ICT	X	X	
Beleidsmedewerker Integrale Veiligheid en Openbare Orde		X	
Chief Information Security Officer	X		
Functioneel beheerder	X		
Functionaris Gegevensbescherming		X	
Gemeentesecretaris	X		
Informatie Adviseur	X		
Juridisch Kwaliteitsadv. Sociaal Domein		X	
Kwaliteitsmedewerker Dienstverlening		X	
Manager Informatie & Bedrijfsvoering	X		
Vertegenwoordiger griffie			X

[2] Met het oog op privacybescherming zijn geen namen opgenomen, alleen functie-aanduidingen.

Geïnterviewde bestuurders en functionarissen	Informatie Beveiliging (A)	Privacy Bescherming (B)	Rol gemeenteraad (C)
Gemeente Nijmegen			
Burgemeester		X	
Portefeuillehouder ICT	X		
Chief Information Security Officer (CISO)	X	X	
Concernmanager Veiligheid, Juridishce Zaken en Bestuursondersteuning	X		
Concernmanager Personeel, Informatie en Facilitair	X		
Functionaris Ggegevensbescherming	X	X	
Functioneel beheerder (2)	X		
Gemeentesecretaris	X		
Informatiecoördinator Zorg- en Veiligheidshuis		X	
Inhoudelijk Coördinator Back Office Wmo/Jeugd		X	
Klachtencoördinator		X	
Kwaliteitsmedewerker Regionaal Ondersteuningsbureau		X	
Manager Basis- en GEO-informatie	X		
Manager Ontwikkel Informatisering en Automatisering (I&A) / Chief Information Officer	X		
Manager Zorg- en Veiligheidshuis		X	
Privacy Officer		X	
Procesmanager Cluster Ondermijning & Informatiegestuurd Werken		X	
Senior Juridisch Beleidsadviseur		X	
Vertegenwoordigers griffie			X

Geïnterviewde bestuurders en functionarissen	Informatie Beveiliging (A)	Privacy Bescherming (B)	Rol gemeenteraad (C)
Gemeente Wijchen			
Burgemeester	X	X	
Portefeuillehouder ICT	X		
Beleidsadviseur Openbare Orde en Veiligheid		X	
Beleidsadviseur Zorg en Veiligheid		X	
Beleidsmedewerker Jeugd, Wmo, Gezondheid		X	
Chief Information Security Officer	X		
Funtionaris Ggegevensbescherming	X	X	
Functioneel beheerder	X		
Gemeentesecretaris	X		
i-adviseur	X		
Kwartiermaker Informatiemanagement	X		
Manager Bedrijfsvoering	X		
Strategisch Informatiemanager	X		
Vertegenwoordiger griffie			X
iRvN			
Lid DB iRvN met ICT-portefeuille	X		
Afdelingshoofd ICT	X		
Afdelingshoofd Informatie- en applicatiebeheer	X		
Lid Cyber Security Incident Response Team	X		
Chief Information Security Officer	X	X	
Coördinator ICT-beheer	X		
Coördinator informatie- en applicatiebeheer (2)	X		
Coördinator informatie- en applicatiebeheer Sociaal Domein	X	X	
Directeur iRvN	X	X	
Security Officer	X		

Van alle gesprekken is een verslag op hoofdlijnen gemaakt, dat voor verificatie is teruggelegd bij de geïnterviewde.

Deelnemers expertmeeting

In de expertmeeting is met (ervarings)deskundigen[3] uit het land gesproken over de (mogelijke) invulling van de kaderstellende en controlerende rol van de gemeenteraad en wat hij daarvoor nodig heeft. Deelnemers aan de expertmeeting waren:

- CISO van een gemeente die recent slachtoffer was van een hack, tevens raadslid en voormalig rekenkamerlid;
- Onafhankelijk toezichthouder naleving AvG, tevens FG in een aantal gemeenten en ondersteuner van de VNG bij AVG-management;
- Deskundige op het gebied van informatiebeveiliging, tevens extern (rekenkamer)onderzoeker;
- Vertegenwoordigers van drie rekenkamers met ervaring met rekenkameronderzoek op het gebied van informatiebeveiliging en privacybescherming en zicht op de verbetertrajecten die naar aanleiding daarvan – mede op basis van besluitvorming door gemeenteraden - gestart zijn;
- Directeur Nederlandse Vereniging van Rekenkamers en Rekenkamercommissies, tevens raadslid.

[3] Met het oog op privacybescherming zijn geen namen opgenomen, alleen functie-aanduidingen.

BIJLAGE 2: NORMENKADER

In deze bijlage is voor de deelvragen die leidend waren bij de uitvoering van het onderzoek aangegeven welke beoordelings- of toetsingsnormen wij daarbij gebruikt hebben:

- Onderzoeksdeel A: informatiebeveiliging;
- Onderzoeksdeel B: privacybescherming;
- Onderzoeksdeel C: de rol van de raad.

Beoordelings- en toetsingsnormen Informatiebeveiliging

In de volgende tabel zijn de beoordelings- of toetsingsnormen voor onderzoeksdeel A (Informatiebeveiliging) opgenomen.

Deelvragen met beoordelings- of toetsingsnormen onderzoeksdeel A. Informatiebeveiliging	
Deelvraag	**Beoordelings- of toetsingsnormen**
A1. Hoe zijn de taken en verantwoordelijkheden op het terrein van ICT- en informatiesystemen en met name de informatiebeveiliging tussen de gemeenten en iRvN verdeeld?	Beschrijvende vraag. Aanvullende norm: is de taakverdeling duidelijk voor de betrokken partijen?
A2. Wat zijn de beleidskaders van de gemeenten en iRvN t.a.v. hun informatiebeveiliging, met name van persoonsgegevens?	Geen normen / beschrijvende vraag.
A3. Voldoen deze beleidskaders aan de gangbare standaarden en wetgeving op het vlak van privacy en informatiebeveiliging?	In algemene zin moet beleid duidelijkheid geven over doelstellingen, middelen en voorziene activiteiten (de 3 W-vragen). Voor het bepalen van het volwassenheidsniveau worden de volgende normenkaders en richtlijnen gehanteerd: - Baseline Informatiebeveiliging Overheid (BIO) - ISO 27001: 2013 - Center for Internet Security (CIS) top 20 (versie 8) - NIST Cybersecurity Framework (CSF) (v1.1) De relevante onderdelen hieruit zijn opgenomen in een afzonderlijke tabel. Dat geldt ook voor de omschrijvingen en criteria voor de verschillende stadia van volwassenheid.
A4. Wat is het beschikbare budget van de deelnemende gemeenten en iRvN voor informatiebeveiliging, en is het mogelijk om een oordeel te geven (bijvoorbeeld door benchmarking) over de toereikendheid hiervan?	- De beschikbare middelen zijn voldoende voor het realiseren van de voorgenomen doelen en activiteiten. - Advies CyberSecurityRaad 2017: 10% van het IT-budget als maatstaf nemen voor digitale veiligheid.

Deelvragen met beoordelings- of toetsingsnormen onderzoeksdeel A. Informatiebeveiliging	
Deelvraag	**Beoordelings- of toetsingsnormen**
A5. In hoeverre worden de beleidskaders in de praktijk in de gemeenten en iRvN nageleefd?	Geen / beschrijvende vraag.
A6. Op welke manier worden gemeentelijke medewerkers bewust gemaakt van hun verantwoordelijkheden ten aanzien van het bewaken van de informatiebeveiliging? Daarbij kan worden gedacht aan onder meer trainingen en ondersteuning, maar ook via functieomschrijvingen, aandacht in functioneringsgesprekken etc.	Voor een goed proces van bewustwording geldt: - De bewustwordingsacties worden gericht ingezet voor de diverse categorieën medewerkers; - De bewustwordingsacties zijn onderdeel van een proces van continu verbeteren (zie A7); - Gegeven de steeds nieuwe veiligheidsdreigingen en – risico's wordt de PDCA-cyclus (ook) met een hoge frequentie doorlopen.
A7. Heeft de gemeente een proces van continu verbeteren in werking voor haar informatiebeveiliging en opslag en beheer van persoonsgegevens in het bijzonder?	Als norm voor een proces van continu verbeteren wordt de toepassing van de PDCA-cyclus (cyclische manier van werken) gehanteerd.
A8. Hebben de gemeenten en iRvN voldoende zicht op de risico's (zowel veiligheidsrisico's als financiële risico's ingeval van lekken of incidenten) op het gebied van informatiebeveiliging, en zijn er maatregelen getroffen om de grootste risico's te kunnen ondervangen?	Voldoende zicht op de risico's betekent: 1. Er is een actuele en volledige risico-inventarisatie; 2. De risico's zijn geanalyseerd op de kans dat deze zich voordoet en het effect daarvan (inhoudelijk en financieel); 3. Voor de risico's is bepaald welke geaccepteerd worden en voor welke maatregelen worden genomen;
A9. Hebben de gemeenten en iRvN een concreet plan voor het effectief en efficiënt verkleinen van de risico's, en voldoet dat plan aan de gebruikelijke standaarden?	In vervolg op de risico-inventarisatie en analyse: 1. Zijn de te nemen maatregelen uitgewerkt in een actieplan. 2. Wordt actief (bij)gestuurd op de uitvoering van het actieplan volgens de principes van de PDCA-cyclus (cyclisch werken).

Volwassenheidsmodel informatiebeveiliging

Voor het bepalen van het volwassenheidsniveau voor informatiebeveiliging is het NBA-LIO en NOREA-volwassenheidsmodel[1] gebruikt. Dit model onderscheid 15 aandachtsgebieden, die een relatie hebben met de volgende normenkader en richtlijnen:

- Baseline Informatiebeveiliging Overheid (BIO)
  De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen de overheid (Rijk, gemeenten, provincies, waterschappen). De BIO is afgeleid van de ISO 27002:2013 norm.
- ISO 27001:2013
  Dit betreft de internationaal erkende norm voor het inrichten, onderhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. De BIO verplicht Nederlandse overheden om het managementsysteem in te richten volgens deze norm.
- Center for Internet Security (CIS) top 20 (versie 8)
  CIS heeft een top 20 'Critical Security Controls' ontwikkeld, waarmee de meest voorkomende cyberaanvullen kunnen worden afgewend.
- NIST Cybersecurity Framework (CSF) (v1.1)
  Framework is een reeks richtlijnen voor het beperken van organisatorische cyberbeveiligingsrisico's, gepubliceerd door het Amerikaanse National Institute of Standards and Technology op basis van bestaande normen, richtlijnen en praktijken. Framework biedt organisaties de mogelijkheid om: 1) hun huidige volwassenheid te bepalen, 2) hun gewenste volwassenheid te bepalen, 3) mogelijkheden voor verbetering en de prioritering daarvan te duiden, 4) voortgang te toetsen en 5) communicatie over informatiebeveiliging te vereenvoudigen.

In de volgende tabel zijn de 15 aandachtsgebieden uit het NBA-LIO en NOREA-volwassenheidsmodel opgenomen en is:

- de korte beschrijving uit het model overgenomen;
- een verwijzing opgenomen naar de bijbehorende normenkaders en richtlijnen;
- een verwijzing opgenomen naar de bijbehorende beheersmaatregel(en) uit het betreffende normenkader of de betreffende richtlijn.

[1] https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

1. Bestuur	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Geeft richting en ondersteuning aan informatiebeveiliging c.q. cyber security in lijn met bedrijfsdoelstellingen, risicobereidheid en van toepassing zijnde wet- en regelgeving en vergewist zich van de effectieve naleving ervan.	BIO (v1.04)	5, 18.2
	ISO 27001 (2013)	5, 6
	CIS top 20 (v8)	18
	NIST CSF (v1.1)	ID.GV
2. Organisatie	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Informatiebeveiliging (inclusief cyber security) is op het hoogst mogelijk organisatieniveau geadresseerd en het beheer van informatiebeveiliging is in lijn met de bedrijfsdoelstellingen en van toepassing zijnde risico's en compliance eisen.	BIO (v1.04)	6
	ISO 27001 (2013)	5.3, 7.1
	CIS top 20 (v8)	-
	NIST CSF (v1.1)	ID.AM
3. Risicobeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het op gestructureerde wijze identificeren en beheersen van informatiebeveiligings- en cyber securityrisico's zodanig dat de risico's in lijn zijn met de risicobereidheid en het risicoraamwerk van de organisatie.	BIO (v1.04)	-
	ISO 27001 (2013)	6, 8.2, 8.3
	CIS top 20 (v8)	-
	NIST CSF (v1.1)	ID.RA
4. Personeelsbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt er zorg voor dat alle medewerkers, inhuurkrachten en derde partijen zich bewust zijn van informatiebeveiligings- en cyber securityrisico's en voldoende geschoold zijn om in lijn met het beveiligingsbeleid hun werkzaamheden te kunnen verrichten.	BIO (v1.04)	7
	ISO 27001 (2013)	7.2, 7.3, 7.4
	CIS top 20 (v8)	14
	NIST CSF (v1.1)	PR.AT
5. Configuratiebeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor de vastlegging en ontsluiting van gegevens over de IT-middelen, IT-koppelingen en IT-diensten.	BIO (v1.04)	8
	ISO 27001 (2013)	-
	CIS top 20 (v8)	1, 2, 4
	NIST CSF (v1.1)	ID.AM

6. Incident/probleembeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het afhandelen van verstoringen in de IT-dienstverlening en voor het tijdig herstellen van de afgesproken dienstenniveaus. Probleembeheer draagt zorg voor het wegnemen of voorkomen van structurele fouten in de IT-dienstverlening.	BIO (v1.04)	16
	ISO 27001 (2013)	9.1, 10.2
	CIS top 20 (v8)	17
	NIST CSF (v1.1)	PR-IP.9, DE-AE.5, RS-AN.2, RS-AN.4, RS-MI, PR-IP.9
7. Wijzigingsbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het beheerst doorvoeren van wijzigingen in IT-middelen, IT-koppelingen en IT-diensten (o.a. applicaties).	BIO (v1.04)	12.1.2
	ISO 27001 (2013)	-
	CIS top 20 (v8)	1, 2, 4
	NIST CSF (v1.1)	PR-IP.3
8. Systeemontwikkeling	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het ontwikkelen van geautomatiseerde oplossingen in lijn met ontwerpspecificaties, ontwikkelen documentatiestandaarden en kwaliteits- en acceptatiecriteria (inclusief wet- en regelgeving).	BIO (v1.04)	14
	ISO 27001 (2013)	-
	CIS top 20 (v8)	16
	NIST CSF (v1.1)	-
9. Gegevensbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het onderhouden van de volledigheid, juistheid, beschikbaarheid en bescherming van gegevens.	BIO (v1.04)	8, 13, 18.1
	ISO 27001 (2013)	-
	CIS top 20 (v8)	3, 11
	NIST CSF (v1.1)	PR.DS, PR.IP
10. Identiteits- en toegangsbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het beheren van de logische toegang tot informatie, informatiediensten (o.a. applicaties) en externe koppelingen.	BIO (v1.04)	9
	ISO 27001 (2013)	-
	CIS top 20 (v8)	5, 6
	NIST CSF (v1.1)	PR-AC

11. Beveiligingsbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het in kaart brengen, adresseren en mitigeren van de risico's van beschikbaarheid, integriteit en vertrouwelijkheid die van toepassing zijn op de informatievoorziening.	BIO (v1.04)	6.2, 9, 10, 12, 13, 14
	ISO 27001 (2013)	-
	CIS top 20 (v8)	7, 8, 9, 10, 12, 13
	NIST CSF (v1.1)	PR.PT, DE-AE, DE-CM, DE.DP,
12. Fysieke beveiliging	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het toegangsbeheer tot ruimtes en de bescherming van personen en objecten tegen incidenten die een fysieke schade aan personen of objecten tot gevolg kunnen hebben.	BIO (v1.04)	11
	ISO 27001 (2013)	-
	CIS top 20 (v8)	-
	NIST CSF (v1.1)	PR-AC.2, PR-AT.5, PR-IP.5, DE-CM.2
13. IT-operatie	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het operationeel houden van de IT-diensten.	BIO (v1.04)	12.1.3, 12.3
	ISO 27001 (2013)	-
	CIS top 20 (v8)	11
	NIST CSF (v1.1)	PR-DS.4, PR-IP.4
14. Bedrijfscontinuïteitsbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het herstellen en voorzetten van de bedrijfsvoering na het optreden van een calamiteit in overeenstemming met de hiervoor afgesproken dienstenniveaus.	BIO (v1.04)	17
	ISO 27001 (2013)	-
	CIS top 20 (v8)	11
	NIST CSF (v1.1)	PR-IP.9, PR-IP.10
15. Ketenbeheer	**Referentie normenkader(s)**	**Referentie beheersmaatregelen**
Draagt zorg voor het bewaken van de levering van de afgesproken dienstverlening door (interne en externe) leveranciers.	BIO (v1.04)	15
	ISO 27001 (2013)	6, 8.2, 8.3
	CIS top 20 (v8)	15
	NIST CSF (v1.1)	ID-BE, ID-AM.6 PR-AT-3

Beoordelings- of toetsingsnormen privacybescherming

In de volgende tabel zijn de beoordelings- of toetsingsnormen voor onderzoeksdeel B (Privacybescherming) opgenomen.

Deelvragen met beoordelings- of toetsingsnormen onderzoeksdeel B. Privacybescherming	
Deelvraag	**Beoordelings- of toetsingsnormen**
B1. Wat zijn de gemeentelijke beleidskaders t.a.v. privacybescherming in het sociaal domein? Hoe wordt er geanticipeerd op de AVG?	1e deel: geen / beschrijvende vraag. 2e deel: er is een implementatieplan gericht op het voldoen aan de regels uit de AVG.
B2. Voldoen deze beleidskaders aan de gangbare standaarden en wetgeving?	Als beoordelings- of toetsingsnorm voor 'gangbare standaarden en wetgeving' zijn de thema's en bijbehorende artikelen uit de AVG gehanteerd. Deze zijn opgenomen in een afzonderlijke tabel.

B3. Hoe is het beleid uitgewerkt en geborgd in processen? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.	Een goede uitwerking en borging betekent:
	- Het beleid is vertaald in activiteiten in een volledig en actueel uitvoeringsprogramma, met per activiteit toegekende:
	  - bevoegdheden en verantwoordelijkheden
	  - beschikbare middelen (personeel en financieel). / Advies CyberSecurityRaad 2017: 10% van het IT-budget als maatstaf nemen voor digitale veiligheid.
	- De uitvoering wordt actief (bijgestuurd) op basis van de principes van de PDCA-cyclus (cyclisch werken).

B4. Hoe is de toegang tot dossiers (autorisaties) geregeld? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.	Een goed geregelde toegang/autorisaties betekent dat toegang tot persoonsgegevens functiegebonden is en gebaseerd is op het 'need to know' principe. En dat er: - een actuele autorisatiematrix voor de belangrijkste applicaties is; - een monitoringsproces is ingericht, waarmee periodiek gecontroleerd wordt of de uitgegeven autorisaties nog actueel zijn; - verwerkersovereenkomsten en/of convenanten zijn afgesloten met ketenpartners, waarin de vereisten en benodigde maatregelen met betrekking tot de gegevensuitwisseling zijn vastgelegd.

Deelvragen met beoordelings- of toetsingsnormen onderzoeksdeel B. Privacybescherming	
Deelvraag	**Beoordelings- of toetsingsnormen**
B5. In hoeverre worden de beleidskaders en vastgestelde processen en regels nageleefd in de praktijk in de gemeenten (en binnen iRvN)? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.	Geen normen / beschrijvende vraag. Kernwoorden bij beschrijving: - opzet – bestaan – werking - situatie in vergelijkbare gemeenten
B6. Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?	Geen normen / beschrijvende vraag. Kernwoorden bij beschrijving: - opzet – bestaan – werking - situatie in vergelijkbare gemeenten
B7. Op welke manier worden burgers geïnformeerd over het gebruik en de verwerking van hun persoonsgegevens?	Geen / beschrijvende vraag. Kernwoorden bij beschrijving: - opzet – bestaan – werking - situatie in vergelijkbare gemeenten
B8. Hoe ziet het toezicht op de omgang met de persoonsgegevens eruit, op papier en in de praktijk? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.	Geen / beschrijvende vraag. Kernwoorden bij beschrijving: - opzet – bestaan – werking - situatie in vergelijkbare gemeenten
B9. Op welke manier worden gemeentelijke medewerkers bewust gemaakt van hun verantwoordelijkheden ten aanzien van het bewaken van de privacy van persoonsgegevens? Daarbij kan worden gedacht aan onder meer trainingen en ondersteuning, maar ook via functie-omschrijvingen, aandacht in functioneringsgesprekken etc.	Voor een goed proces van bewustwording geldt: - de bewustwordingsacties worden gericht ingezet voor de diverse categorieën medewerkers; - de bewustwordingsacties zijn onderdeel van een proces van continu verbeteren (zie A7); - gegeven de steeds nieuwe veiligheidsdreigingen en – risico's wordt de PDCA-cyclus (ook) met een hoge frequentie doorlopen.
B10. In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom de bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds?	Een goede balans betekent: - aandacht voor mogelijke tegenstellingen tussen regels en procedures rondom de bescherming van privacy en een goede dienstverlening in het privacybeschermingsbeleid en de vertaling daarvan naar de uitvoering; - het actief uitdragen van het privacybeschermingsbeleid van bovenaf in de organisatie; - een hoge mate van bewustzijn onder medewerkers (zie B9); - een goede informatieverstrekking aan burgers; - het bieden van een platform aan burgers om de privacyrechten uit te kunnen oefenen; - dat het zoeken daarnaar onderdeel is van een continu proces van verbeteren (zie A7).

Volwassenheidsmodel Privacybescherming

Voor het bepalen van het volwassenheidsniveau voor privacybescherming is de Privacy Baseline (versie 3.3) van het Centrum Informatiebeveiliging en Privacybescherming (CIP) gehanteerd. Deze Privacy Baseline is gebaseerd op de AVG, de basiswet die sinds 25 mei 2018 in de hele Europese Unie het verzamelen, verwerken en beveiligen van persoonsgegevens regelt. In onderstaande tabel zijn de 13 thema's uit de Privacy Baseline opgenomen en is:

- de korte beschrijving uit de Privacy Baseling overgenomen;
- een verwijzing opgenomen naar de bijbehorende artikelen uit de AVG.

1. Privacybeleid	**Artikel AVG**
De organisatie heeft een privacybeleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen	5, 24, 40
2. Organisatie	**Artikel AVG**
Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG. Daarnaast omvat het thema organisatie ook de bewustwording op de werkvloer van het bestaan van privacy, de privacyregels en hoe dit intern is georganiseerd.	5, 37, 38, 39
3. Risicobeheer	**Artikel AVG**
Beoordeling van de privacy risico's (de kans en hun potentiële omvang/impact) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de organisatie acceptabel acht. De verwerkingsverantwoordelijke neemt passende technische en organisatorische maatregelen om de waarborgen van de AVG in de verwerking in te bouwen.	24, 25, 35, 36, 42
4. Doelbinding gegevensverwerking	**Artikel AVG**
De verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk omschreven: de doeleinden en de rechtvaardigingsgronden.	5, 6, 9, 10, 22, 23
5. Register van verwerkingsactiviteiten	**Artikel AVG**
De verwerkingsverantwoordelijke en de verwerker hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.	30

6. Kwaliteitsmanagement	**Artikel AVG**
De verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Als dit op verzoek van betrokkene gebeurt wordt deze over de status van de afhandeling geïnformeerd.	7 lid 3, 11 lid 2, 12, 16, 17, 18, 19, 20, 21, 22, 23
7. Beveiligen van de verwerking van persoonsgegevens	**Artikel AVG**
Elke organisatie die persoonsgegevens verwerkt dient passende technische en organisatorische maatregelen te nemen om de veiligheid van de persoonsgegevens te waarborgen.	26, 28 en 32
8. Informatieverstrekking aan betrokkenen bij verzameling persoonsgegevens	**Artikel AVG**
De verwerkingsverantwoordelijke stelt bij elke verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor de verwerking.	12, 13, 14, 15
9. Bewaren van persoonsgegevens	**Artikel AVG**
Door het treffen van de benodigde maatregelen hanteert de organisatie voor persoonsgegevens bewaartermijnen die niet worden overschreden.	5
10. Doorgifte persoonsgegevevens	**Artikel AVG**
Bij doorgifte aan een andere verwerkingsverantwoordelijke zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn er afdoende garanties. Bij de doorgifte naar landen buiten de EU: • is er een vertegenwoordiger, en; • is geen sprake van uitzonderingsgronden en; • geldt een door de Europese Commissie genomen adequaatheidsbesluit, of; • zijn er passende waarborgen, of; • geldt een afwijking voor een specifieke situatie.	26, 27, 28, 29, 44, 45, 46, 47, 48, 49, 96
11. Intern toezicht	**Artikel AVG**
Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.	5, 37, 38, 39
12. Toegang gegevensverwerking voor betrokkene	**Artikel AVG**
De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.	11, 12, 15, 22 en 86

13. Meldplicht datalekken	**Artikel AVG**
De verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de AP, documenteert de inbreuk en informeert de betrokkene. Tenzij hiervoor een uitzondering geldt.	33, 34

Stadia van volwassenheid: omschrijving en indicatieve criteria

Op basis van de geanalyseerde documenten en gevoerde gesprekken hebben de externe onderzoekers een inschatting gemaakt van het volwassenheidsniveau van de gemeenten en iRvN per aandachtsgebied (informatiebeveiliging) en thema (privacybescherming).
Volwassenheidsniveau 1 is het laagste en volwassenheidsniveau 5 het hoogste niveau. De onderscheiden niveaus zijn in onderstaande tabel toegelicht.

Niveau	Omschrijving	Indicatieve criteria
1. Ad-hoc	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte beheersmaatregelen geïmplementeerd • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2. Beheerst	Beheermaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Beheersmaatregelen zijn geïmplementeerd • Uitvoering is consistent en standaard • Ad-hoc en grotendeels gedocumenteerd
3. Vastgesteld	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Beheersmaatregel gedefinieerd op basis van risico assessment • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken eenduidig toegewezen • Opzet, bestaan en effectieve werking aantoonbaar • Rapportage van uitvoering van beheersmaatregelen aan management • Effectieve werking van beheersmaatregelen wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie • De toetsing toont aan dat de beheersmaatregel effectief is
4. Voorspelbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.	• Periodieke (beheersmaatregel) evaluatie en opvolging vindt plaats • Evaluatie is gedocumenteerd en geformaliseerd • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de organisatie en is minimaal jaarlijks • Rapportage van de evaluatie aan management

Niveau	Omschrijving	Indicatieve criteria
5. Geoptimaliseerd	De beheermaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continue evalueren van de beheersmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit self-assessments, gap- en root cause analyses • De getroffen beheersmaatregelen worden gebenchmarkt en zijn 'best practice' in vergelijking met andere organisaties • Real time monitoring • Inzet automated tooling

Beoordelings- of toetsingsnormen kaderstellende en controlerende rol van de raad

In de volgende tabel zijn de beoordelings- of toetsingsnormen voor onderzoeksdeel C opgenomen (de kaderstellende en controlerende rol van de raad).

Deelvragen met beoordelings- of toetsingsnormen voor onderzoeksdeel C. Kaderstelling en controle door de gemeenteraden	
Deelvraag	**Beoordelings- of toetsingsnormen**
C1. Op welke wijze verloopt het proces van kaderstelling en controle door de gemeenteraden tot op heden t.a.v. de informatiebeveiliging en privacybescherming in hun gemeente, en hoe moet dit proces en het resultaat ervan worden beoordeeld?	Deels beschrijvende, en deels beoordelende vraag. - Geven de gemeenteraden daadwerkelijk invulling aan hun kaderstellende rol, dat wil zeggen het vaststellen van de hoofdlijnen van het beleid? - Geven de gemeenteraden daadwerkelijk invulling aan hun controlerende rol, dat wil zeggen het controleren of het beleid is uitgevoerd binnen de gestelde kaders?
C2. Op welke wijze faciliteren de colleges de kaderstelling en controle door de gemeenteraden, met name ten aanzien van de informatievoorziening aan de raden?	Deels beschrijvende, en deels beoordelende vraag. - Doen de colleges voldoende in termen van hun passieve en actieve informatieplicht jegens de raden? Actieve informatieplicht = verstrekken van alle informatie, die de raad nodig heeft voor de uitoefening van zijn taken.
C3. Welke voorwaarden en vereisten kunnen worden geïdentificeerd om de kaderstelling en controle beter te laten verlopen? In het bijzonder moet daarbij aandacht zijn voor de inrichting van de informatievoorziening.	Geen normen / beschrijvende vraag.
C4. Zijn er elders in het land relevante best practices ten aanzien van een goed verlopend proces van kaderstelling en controle door de gemeenteraad op dit gebied, en wat zijn de belangrijkste lessen die daaruit kunnen worden geleerd?	Geen normen / beschrijvende vraag.

BIJLAGE 3: 10 BESTUURLIJKE PRINCIPES VOOR INFORMATIEBEVEILIGING VNG RESOLUTIES DIGITALE VEILIGHEID (2021) EN INFORMATIEBEVEILIGING (2013)

In deze bijlage zijn achtereenvolgens de hoofdlijnen opgenomen uit:

- de 10 bestuurlijke principes voor informatiebeveiliging;
- VNG-resolutie digitale veiligheid (2021);
- VNG-resolutie informatiebeveiliging (2013).

10 bestuurlijke principes voor informatiebeveiliging

In 2019 heeft de VNG 10 bestuurlijke principes voor informatiebeveiliging benoemd. Het gaat om een aanvulling op de BIO voor bestuurders. In deze bijlage hebben wij de 10 principes en de toelichting daarop opgenomen. In het document met de 10 bestuurlijke principes wordt per principe ook nog ingegaan op de rol van bestuurders bij het borgen van informatiebeveiliging. Voor het gehele document verwijzen wij naar de betreffende webpagina van de VNG.

1. **Bestuurders bevorderen een veilig cultuur**
   Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.
2. **Informatiebeveiliging is van iedereen**
   Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.
3. **Informatiebeveiliging is risicomanagement**
   Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.
4. **Risicomanagement is onderdeel van de besluitvorming**
   Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.
5. **Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking**
   Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.
6. **Informatiebeveiliging is een proces**
   Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.
7. **Informatiebeveiliging kost geld**
   Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

8. **Onzekerheid dient te worden ingecalculeerd**
   De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.
9. **Verbetering komt voort uit leren en ervaring**
   Risicobeheer wordt voortdurend verbeterd door leren en ervaring.
10. **Het bestuur controleert en evalueert**
    Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

VNG-resolutie digitale veiligheid (2021)

Op 12 februari 2021 is de resolutie 'Digitale Veiligheid: kerntaak voor gemeenten' unaniem aangenomen door de leden van de VNG. In de resolutie worden de leden van de VNG opgeroepen:

- incidenten te delen met de IBD wanneer een dergelijk incident ook zou kunnen optreden bij andere gemeenten en / of andere sectoren;
- jaarlijks een incidentoverzicht op categorieniveau te delen met de IBD, zodat een compleet inzicht bestaat van dreigingen, trends en ontwikkelingen;
- een digitaal incidentbestrijdingsplan vast te stellen en jaarlijks te actualiseren;
- invulling te geven aan de noodzakelijke intergemeentelijke solidariteit bij (gemeentelijke) digitale incidenten mede op aangeven van de Informatiebeveiligingsdienst;
- periodiek te oefenen met cyberincidenten om daarmee de gemeentelijke weerbaarheid te toetsen en te vergroten;
- periodiek het onderwerp digitale veiligheid in het college van B&W te agenderen;
- in de Integrale Veiligheidsplannen ook de digitale aspecten expliciet te benoemen:
  - de veiligheid van de samenleving bij het optreden van digitale incidenten;
  - het voorkomen en bestrijden van cybercriminaliteit;
  - het beveiligen van de informatie waarvoor zij verantwoordelijkheid draagt.

De tekst van de hele resolutie is te lezen via de hiervoor opgenomen link.

VNG-resolutie informatieveiligheid (2013)

Op 29 november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen door de leden van de VNG. In de resolutie hebben de leden van de VNG ingestemd met de volgende punten:

1. Informatieveiligheid wordt onderdeel van de collegeambities 2014-2018 en wordt opgenomen in de portefeuille van een van de leden van het college van B&W.
2. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.

3. Gemeenten stellen de Baseline Informatiebeveiliging Gemeenten vast als hét gemeentelijke basisnormenkader voor informatieveiligheid.
4. Gemeenten stellen informatieveiligheidsbeleid vast aan de hand van de Baseline Informatiebeveiliging Gemeenten.
5. Uitvoering van dat beleid wordt gebaseerd op eigenstandige risicoafwegingen. Gemeenten zijn zich daarbij bewust van de (continu veranderende) informatieveiligheidsrisico's die ze lopen en nemen hierop adequate maatregelen.
6. Gemeenten borgen informatieveiligheid bestuurlijk en organisatorisch door aansluiting in de reeds bestaande planning- en controlcyclus. Gemeenten creëren hiernaast, door middel van leren en ontwikkelen, blijvend bewustzijn op informatieveiligheid.
7. Gemeenten maken de lokale invulling rondom het thema van informatieveiligheid transparant voor burgers, bedrijven en (keten)partners. Deze transparantie wordt ondermeer behaald door gebruik te maken van waarstaatjegemeente.nl. Deze openbare informatie vormt de basis voor jaarlijkse collegiale beoordeling (peer reviews). Daarnaast toetst een interbestuurlijke visitatiecommissie, tenminste eens in de vijf jaar, of het systeem van 'verplichtende zelfregulering' voldoende werkt.

Daarnaast hebben de leden met het vaststellen van de resolutie een aantal opdrachten aan het bestuur van de VNG gegeven. De tekst van de hele resolutie is te lezen via de hiervoor opgenomen link.

BIJLAGE 4: OVERZICHT 60 VERPLICHTE BIO-DOCUMENTEN

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen de overheid (Rijk, provincies, gemeenten, waterschappen). De BIO vervangt voor gemeenten de sinds 2012 geldende Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Afgesproken is dat alle overheidslagen 2019 als overgangsjaar zouden gebruiken voor de implementatie van de BIO en dat ze deze vanaf 1 januari 2020 verplicht hanteren. Op basis van de BIO dienen overheden te beschikken over de volgende 60 verplichte documenten:

#	Referentie normenkader ISO 27001[1]	Referentie beheersmaatregel
1	4.3	Toepassingsgebied van het ISMS
2	5.2	Informatiebeveiligingsbeleid
3	6.1.2	Risicobeoordelingsprocedure
4	6.1.3	Risico Behandelprocedure
5	6.2	Informatiebeveiligingsdoelstellingen
6	7.2	Competenties
7	7.5.1	Informatie noodzakelijk voor de doeltreffendheid van het ISMS
8	7.5.3	Informatie van externe oorsprong nodig voor de planning en uitvoering van het ISMS
9	8.1	Informatie die nodig is om te zien dat de processen volgens planning zijn uitgevoerd
10	8.2	Resultaten van de risicobeoordelingen
11	8.3	Rapport risicobehandeling
12	9.1	Resultaten van het monitoren en meten
13	9.2	Interne auditprogramma en de auditresultaten
14	9.3	Resultaten van de directiebeoordeling
15	10.1	Afwijkingen, de genomen maatregelen en het resultaat van de maatregelen
16	A.6.1.1	Rollen en verantwoordelijkheden voor IB
17	A.6	Governance en rapportagelijn
18	A.6.2.1.	Beleid voor mobiele apparatuur
19	A.6.2.2	Beleid voor telewerken

[1] De BIO is gebaseerd op de ISO 27001. Zie bijlage 2 voor een nadere toelichting.

#	Referentie normenkader ISO 27001	Referentie beheersmaatregel
20	A.6.1.5	Informatiebeveiliging in projecten
21	A.7.1.1	Screening
22	A.7.2.2	Training en awareness
23	A.8.1.1	Inventariseren van bedrijfsmiddelen
24	A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen
25	A.8.2.2	Procedure informatie labelen en classificatie
26	A.8.2.3	Procedures voor het behandelen van bedrijfsmiddelen
27	A.8.3.1	Procedure beheer van verwijderbare media
28	A.9.1.1	Beleid voor toegangsbeveiliging
29	A.9.1.2	Registratie- en uitschrijvingsprocedure voor toegangsrechten
30	A.9.2.2	Gebruikerstoegangsverleningsprocedure
31	A.9.2.4	Beheersproces voor het beheer van geheime authenticatie- informatie van gebruikers
32	A.9.4.2	Beveiligde inlogprocedures
33	A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen
34	A.10.1.2	Beleid m.b.t. sleutelbeheer
35	A.11	Fysiek beleid inclusief zonering
36	A.11.1.5	Procedure werken in beveiligde gebieden
37	A.11.2.9	‘Clear desk’- en ‘clear screen’-beleid
37	A.12.1.2	Wijzigingsbeheer
39	A.12.3.1	Backup beleid
40	A.12.1.1	Gedocumenteerde bedieningsprocedures
41	A.12.4.1	Logbestanden van gebeurtenissen
42	A.12.4.3	Logbestanden van beheerders en operators
43	A.12.5.1	Procedure software installeren op operationele systemen
44	A.12.6	Patchmanagement
45	A.12.6	Kwetsbaarhedenbeheer
46	A.13.2.1	Beleid en procedures voor Informatietransport
47	A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst

#	Referentie normenkader ISO 27001	Referentie beheersmaatregel
48	A.14.2.1	Beleid voor beveiligd ontwikkelen
49	A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen
50	A.14.2.5	Principes voor engineering van beveiligde systemen
51	A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties
52	A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
53	A.16.1.1	Verantwoordelijkheden en procedures m.b.t. incidenten
54	A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
55	A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging
56	A.16.1.5	Respons op informatiebeveiligingsincidenten
57	A.16.1.7	Procedure verzamelen van bewijsmateriaal
58	A.17.1.2	Informatiebeveiligingscontinuïteit implementeren
59	A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen
60	A.18.1.2	Procedure intellectuele eigendomsrechten

BIJLAGE 5: STRATEGISCHE, TACTISCHE EN OPERATIONELE KADERS UIT DE BASISAFSPRAKEN ICT-DIENSTEN

De dienstverlening van iRvN aan de deelnemende gemeenten is vastgelegd in het document 'Basisafafspraken ICT-diensten' (verder: Basisafspraken)[1]. Daarin zijn ook strategische-, tactische en operationele kaders opgenomen. De aard van de kaders is in de Basisafspraken als volgt toegelicht:

- De *strategische kaders* zijn algemeen van aard, bestrijken een langere periode (vier tot vijf jaar) en vragen besluitvorming/bepaling door bestuurders;
- De *tactische kaders* zijn een uitwerking van de strategische kaders, zijn gesteld in heldere afspraken over het handelen die gemanaged kunnen worden en bestrijken een kortere periode (één tot drie jaar);
- De *operationele kaders* betreffen de uitvoering, het 'doen', en zijn concreet verwoord.

In deze bijlage zijn de strategische kaders overgenomen. Om een indruk te krijgen, is ook een aantal tactische en operationele kaders opgenomen.

Strategische kaders

1. We werken samen, tenzij…[2];
2. We zetten in op optimale inzet van binnen de regio beschikbare ICT-middelen, met het oog op bedrijfscontinuïteit;
3. We werken onder architectuur, zoals gemeentelijk architectuur, GEMMA[3] en NORA[4];
4. We sluiten aan bij landelijke ontwikkelingen, wettelijke ontwikkelingen, programma's (zoals Open Overheid) en plannen etc, tenzij…;
5. iRvN is het samenwerkingsplatform op het gebied van technologische ICT-innovaties en landelijke, Europese ICT-programma's;
6. We streven naar gemeenschappelijk opdrachtgeverschap van gemeenten naar iRvN.

[1] Voor dit onderzoek is de versie van de Basisafspraken bestudeerd die gelden vanaf 1 januari 2021.

[2] Bij twee strategische kaders is een 'tenzij' opgenomen. Daarbij is toegelicht dat het voor een gemeente mogelijk moet zijn om een afwijkende keuze te maken. Samenwerking is een (zwaarwegende) intentie genoemd, niet een verplichting. Aangegeven is dat afwijkingen geen probleem hoeven te zijn zolang beargumenteerd afgeweken wordt.

[3] Voor een toelichting op GEMMA: https://www.gemmaonline.nl/index.php/Gemeentelijke_Model_Architectuur_(GEMMA)

[4] Voor een toelichting op NORA: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/standaardisatie-en-architectuur/nora/

Tactische kaders

Om een indruk te krijgen zijn hierna enkele voorbeelden van tactische kaders uit de Basisafspraken opgenomen. Het nummer achter het voorbeeld verwijst naar het strategisch kader waar het tactische kader een uitwerking van is.

- voor het kantoor-automatiseringsbeleid stellen we gezamenlijke uitgangspunten vast (1);
- de werkplek is AVG/BIO-compliant (2)[5];
- iRvN is voorbereid op de implementatie van 'Common Ground'[6] infrastructuur (3 en 4);
- iRvN blijft haar personeelbestand kwalitatief en kwantitatief ontwikkelen in lijn met de landelijke en technologische ontwikkelingen en kaders (5);
- we dragen gezamenlijk verantwoordelijkheid voor de naleving van privacy- en informatieveiligheid (6).

Operationele kaders

Om een indruk te krijgen zijn hierna enkele voorbeelden van operationele kaders uit de Basisafspraken opgenomen. Het nummer achter het voorbeeld verwijst naar het strategisch kader waar het operationele kader aan gekoppeld is.

- we brengen gezamenlijk een prioritering aan in de projecten die in een jaar worden uitgevoerd (1 en 2);
- alle data-uitwisseling tussen informatiesystemen loopt altijd via iRvN-ESB[7] (3);
- als wij MFP's[8] moeten vernieuwen, besteden we landelijk aan, tenzij er reden is dit niet te doen (4);
- iRvN ondersteunt de gemeenten tijdig en pro-actief bij toekomstige maatschappelijke, technologische en wettelijke ontwikkelingen (5);
- we stellen jaarlijks samen de Productcatalogus vast die leidend is voor de standaard-dienstverlening (6).

[5] AVG: Algemene verordening gegevensbescherming. BIO: Baseline Informatiebeveiliging Overheid.

[6] Voor een toelichting op 'Common Ground': https://www.vngrealisatie.nl/roadmap/common-ground

[7] ESB: Een Enterprise Service Bus (ESB) is een software oplossing waarmee de onderlinge communicatie wordt uitgevoerd voor allerlei verschillende bedrijfssystemen binnen een organisatie.

[8] MFP: multifunctionele printer.

BIJLAGE 6: VOORBEELD VAN RAPPORTAGE AAN DE GEMEENTERAAD

In deze bijlage is een voorbeeld opgenomen van een rapportage aan de gemeenteraad voor privacybescherming: het jaarverslag van de Functionaris Gegevensbescherming (FG) van de gemeente Hilversum. De FG van de gemeente Hilversum stelt jaarlijks een compact jaarverslag op. De kern hiervan vormen de 'bestuurlijke ontwikkellijn' en de 'ontwikkellijn per aandachtsgebied'. Aan de hand van een compacte set prestatie-indicatoren en met behulp van symbolen wordt voor beide lijnen op één A4 inzichtelijk gemaakt hoe ver de gemeente is. Daarbij geeft de FG ook steeds een advies. Aan de hand van de scores op de bestuurlijke ontwikkellijn, drukt de FG in één cijfer uit of de sturing op niveau is en, zolang dat nog niet zo is, of er een (voldoende) stijgende lijn te zien in. De gemeenteraad bespreekt het jaarverslag.

In de gemeente Amersfoort wordt een ENSIA-verantwoording van het college aan de raad ontwikkeld met een vergelijkbare opzet: in die rapportage worden met behulp van indicatoren en symbolen onder andere de stand van zaken voor de verschillende BIO-domeinen en de landelijke voorzieningen toegelicht. Op dit moment (1 juli 2022) is deze rapportage nog niet openbaar.

FG-verslag 2020-2021

Aan: het college van B&W Gemeente Hilversum
Van: de functionaris gegevensbescherming

Inleiding

Sinds de invoering van de AVG in 2018, is de functionaris voor gegevensbescherming (FG) voor gemeenten de toezichthouder op de naleving van de AVG, gerelateerde wetgeving en beleids-afspraken. De FG adviseert de gemeente en brengt rechtstreeks verslag uit aan het college.[1]

Doel van de AVG is de bescherming van *personen* bij verwerking van persoonsgegevens ('mens centraal') en niet zozeer de bescherming van gegevens.[2] Dat maakt wezenlijk verschil. Toch wordt in ons land vaak de nadruk gelegd op gegevensbescherming, met als gevolg dat de AVG onnodig restrictief wordt uitgelegd of zich problemen kunnen voordoen zoals de Toeslagenaffaire.

FG's hebben eraan bij te dragen dat de AVG conform de bedoeling wordt gehanteerd. Onder het FG-toezicht vallen zowel binnen- als buitengemeentelijke vormen van gegevensverwerking. Zo heeft Gemeente Hilversum taken op het gebied van jeugd en gezin opgedragen aan de gemeenschappelijke regeling Gooi en Vechtstreek. U blijft als college voor de AVG eindverantwoordelijk en aansprakelijk, mochten inwoners problemen ondervinden door de gegevensverwerking binnen dit samenwerkingsverband.[3]

De AVG prevaleert boven nationale wet- en regelgeving en reguleert het vermogen van de gemeente om persoonsgegevens te mogen verwerken of dit uit te besteden. Hiervoor bevat de AVG voorwaarden in de vorm van kwaliteitseisen, transparantieverplichtingen en dienstverlenings-voorschriften zoals facilitering van individuele inzage- en correctiemogelijkheden. Door te handelen naar deze voorwaarden, bewerkstelligt u het groene licht van de AVG.

Beoordeling AVG-naleving

Groen licht veronderstelt een volwassen digibewuste cultuur.[4] Zover zijn gemeenten vaak nog niet en Hilversum vormt geen uitzondering. Om uw ontwikkeling inzichtelijk te maken, introduceerde ik in 2018 de dashboardrapportages die u aantreft op pagina's 6 en 7 van dit verslag.

- *De bestuurlijke ontwikkellijn* is meest wezenlijk omdat hieruit blijkt in hoeverre de gemeente beschikt over het vermogen om bescherming van persoonsgegevens duurzaam te waarborgen.
- *De ontwikkellijn per aandachtsgebied* gaat over de vraag in hoeverre u erin slaagt om ook groen licht te verdienen op uitvoeringsniveau.

[1] Artikel 37-39 AVG.

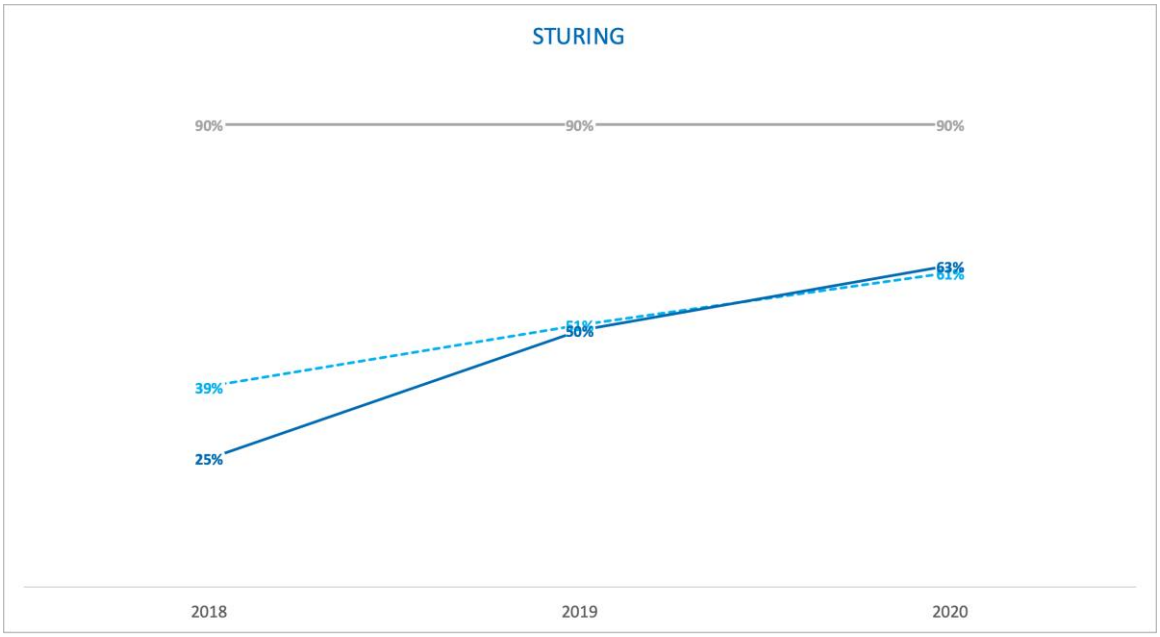
[2] Artikel 1 AVG - waarbij aangetekend dat het niet alleen gaat om bescherming van de persoon in kwestie maar ook om de bescherming van anderen zoals bijvoorbeeld omwonenden.

[3] EU/EDPB *Guidelines on the concepts of controller and processor*, 07/2020.

[4] Het tegenovergestelde van digibetocratie.

Naleving van de AVG is iets kwalitatiefs en laat zich niet gemakkelijk in een cijfer uitdrukken. Toch stelt met name de bestuurlijke ontwikkellijn in staat om een beoordeling af te geven, door de vraag te stellen in hoeverre het beleidsthema de aandacht krijgt die het verdient. Het is welbegrepen dat er andere beleidsthema's zijn die belangrijk zijn, maar dat neemt niet weg dat de aandacht voor bescherming van personen bij gegevensverwerking 100% behoort te zijn, of in ieder geval meer dan 90%.[5]

Voor Gemeente Hilversum bedroeg dat percentage 2018 en 2019 nog 25% respectievelijk 50%, in 2020 is dit verder gestegen naar 63%. Dat is een opgaande lijn. De bestuurlijke ontwikkellijn had wellicht een steiler verloop gehad als in 2020 de coronacrisis niet was uitgebroken.



Verloop bestuurlijke ontwikkellijn – de donkerblauwe lijn geeft de AVG-beleidsvoering van Gemeente Hilversum weer. De lichtblauwe stippellijn toont het gemiddelde van gemeenten waar PMP het FG-schap invult. Sturing boven de 90% wil zeggen dat bestuur en management 'op niveau' zitten. Het vergt tijd en inspanningen om op dat niveau te komen en niet terug te vallen.

Opvallend in 2020

Vooral positief is dat er sprake is van een stijging, óndanks de coronacrisis. Dit wordt met name verklaard doordat het interne supportteam voor AVG en informatiebeveiliging, het PIT, werd versterkt met extra mensen waardoor meer werk verzet kan worden en uitval niet meteen leidt tot stilstand in de beleidsvoering.

Door in 2021 de juiste prioriteiten te stellen en resultaten te boeken, moet het mogelijk zijn om in 2021 de ontwikkellijn steilere stijging te geven. Twee invalshoeken werken bevorderend:

- de ontwikkeling van een bestuurlijke visie op 'Hilversum 2035': wat wil de gemeente betekenen voor haar inwoners in het digitale tijdperk en hoe organiseer je dat slim – ook in samenwerking met regionale en landelijke ketenpartners?
- bestuurlijke aandacht voor digitale transformatie tijdens collegevergaderingen, raadsvergaderingen en in het directieteam.

[5] De percentages zijn het gemiddelde van de scores in de kolom 'werking' op de bestuurlijke ontwikkellijn in de FG-verslagen 2018-2020.

In 2020 is het PIT er in geslaagd om zich beter binnen de gemeenteorganisatie te manifesteren. De managementrapportages van het PIT maken de voortgang inzichtelijk. De privacy officers slagen er steeds beter in om proceseigenaren klantgericht te ondersteunen en oogsten op die manier waardering.

Hét instrument om tot een AVG-conforme werkwijze te komen, is de uitvoering van *dataprotectie impact assessments* (DPIA's). Een goede DPIA doet denken aan een milieueffectentoets, maar voor de digitale leefomgeving. De proceseigenaar onderzoekt, geholpen door het PIT, welke risico's personen lopen zónder beschermingsmaatregelen en welke maatregelen nodig zijn om effectieve bescherming te bieden zodat die risico's zich redelijkerwijs niet kunnen voordoen.

In het afgelopen jaar zijn verschillende DPIA's opgestart, zoals de DPIA Ondermijning en een DPIA Werk en Inkomen, naast de DPIA's die zijn uitgevoerd voor smart city-projecten (Snelliuslaan, Druktemeter, Hoppler buurtplatform) en bijvoorbeeld de DPIA bodycams.

Het is aan het PIT om te rapporteren over voortgang en resultaten volgens het jaarplan dat in samenspraak met het college is vastgesteld. Belangrijk is dat met de uitvoering van DPIA's in het afgelopen jaar kennis en ervaring is opgedaan, waardoor Gemeente Hilversum nu beter kan voorzien in passende maatregelen zoals de AVG voorschrijft.

Medewerkers en bestuurders worden uitgedaagd om kritischer te zijn, onder meer op protocollen en regelingen waarmee ogenschijnlijk de AVG wordt nageleefd. Een voorbeeld is de 'Verwerkersovereenkomst Machtigingsbesluit Toeslaggedupeerden' die eind 2020 tot stand kwam. Bij toetsing aan de AVG bleek deze regeling in het geheel niet te kloppen omdat geen rekening was gehouden met de eigen verantwoordelijkheid van gemeenten.[6]

FG-advies voor 2021

In de rechterkolom van de bestuurlijke ontwikkellijn en de ontwikkellijn per aandachtsgebied treft u aanbevelingen aan voor een verdere opgaande lijn in 2021. Hoofdzakelijk gaat het om het volgende:

1. Leg de nadruk op realisatie van beheersmaatregelen. Geef proceseigenaren duidelijk opdracht en laat hen verantwoording afleggen over genomen beschermingsmaatregelen. Bij hogere risicoscores (zie privacybeleidskader) zijn proceseigenaren ook opdrachtgever van audits.
2. Ontwikkel een eigen bestuurlijke visie en strategie op de digitalisering en de opkomst van nieuwe technologieën zoals smart tech, algoritmes en kunstmatige intelligentie. Hanteer de AVG als kompas om te waarborgen dat gegevensverwerking ten dienste staat van de mens.
3. Maak met buurgemeenten en ketenpartners afspraken over ieders rol en verantwoordelijkheid in informatieketens.

Meer specifiek verdienen in 2021 schuldhulpverlening en het werk van bijzondere opsporingsambtenaren aandacht. Het PIT heeft in het werkplan 2021 aangegeven hier werk van te maken.

- Schuldhulpverlening vanwege de recente wijziging van de Wet gemeentelijke schuldhulpverlening waarin wordt benadrukt dat gegevens kunnen worden gedeeld voor een meer menscentrale aanpak. Door de coronacrisis en de toeslagenaffaire is dat actueel.
- Het werk van bijzondere opsporingsambtenaren verdient prioriteit omdat op de verwerking van persoonsgegevens door BOA's sinds 2018 vaak óók vernieuwde Wet politiegegevens van toepassing is. Bij de aanpassing van de Wpg is bepaald dat op de gegevensverwerking door

[6] De verwerkersovereenkomst is door het Ministerie van Financiën voorgesteld aan gemeenten, in samenwerking met de VNG.

BOA's na twee jaar een audit dient te worden uitgevoerd, die daarna om de vier jaar moet worden herhaald.

Bijdrage FG aan de beleidsvoering

Als FG ondersteun ik de beleidsvoering vanuit mijn wettelijke rol en verantwoordelijkheid. Ik kan helpen door misverstanden over de AVG weg te nemen en de baten van duurzaam databeleid te accentueren. Via participatie in regionaal FG-overleg en bijvoorbeeld mijn contacten met de Autoriteit Persoonsgegevens help ik het pad te effenen voor toekomstvast gemeentebestuur. Uw FG is ook degene die als de gemeentelijke data-ombudsman de personen helpt die ondanks alle waarborgen op het gebied van gegevensbescherming, toch verstrikt raken of in de steek zijn gelaten door 'het systeem' waar Gemeente Hilversum evenzeer deel van uit maakt.

Utrecht, 10 maart 2021



Mr. S.H. Katus, CIPP/E CIPM FIP

Leeswijzer ontwikkellijnen

Algemeen

In de kern gaat de AVG niet over privacy. De AVG reikt praktische handvatten aan voor maatschappelijk verantwoord omgaan met persoonsgegevens, duurzame samenwerking binnen informatieketens (jeugdketen, zorgketen, veiligheidsketen, ...) en acceptabele inzet van nieuwe technologieën zoals data-analyse, algoritmes / kunstmatige intelligentie, gezichtsherkenning, drones of bijvoorbeeld verkeerssensoren.

Voor de beoordeling van de mate waarin een gemeente aan de AVG voldoet, hanteer ik hierna zowel prestatie-indicatoren op bestuurlijk niveau (bestuurlijke ontwikkellijn) als prestatie-indicatoren op uitvoeringsniveau (ontwikkellijn per aandachtsgebied).[7] De kwaliteit van de beleidsvoering visualiseer ik vervolgens zowel aan de hand van onderstaande symbolen, als de driedeling 'opzet, bestaan en werking'.



Niet onderzocht, afwezig of niet aantoonbaar	In aanzet aanwezig en aantoonbaar	Substantieel aanwezig en aantoonbaar	Grotendeels aanwezig en aantoonbaar	Volledig aanwezig en aantoonbaar	Onderzocht maar (nu) niet aan de orde.

- **Opzet:** de aanpak klopt op papier – er is goed over nagedacht.
- **Bestaan:** de aanpak is volgens plan in praktijk gebracht – de gemeente heeft daadwerkelijk in passende gegevensbescherming voorzien.
- **Werking:** de aanpak blijkt ook in de praktijk doelmatig en doeltreffend.

Control & accountability

Overal zou een 100% score moeten staan, uitgezonderd situaties waarin de AVG niet van toepassing is omdat (nog) niet met persoonsgegevens wordt gewerkt. Daarmee is niet gezegd dat oplossingen perfect zijn of dat zich geen privacydiscussies kunnen voordoen, maar wel dat de gemeente naar behoren de AVG naleeft, doordat is voorzien in AVG-conforme oplossingen ('passende maatregelen'). Het gemeentebestuur (vooral het college), is dan maximaal *in control* en in de positie om met vertrouwen verantwoording af te leggen over beleid en maatregelen

- Dit FG-verslag ondersteunt de verantwoording door het college aan de raad en eventueel anderen, zoals de Autoriteit Persoonsgegevens of de rechter.
- De raad beschikt aan de hand van dit verslag over de informatie die nodig is om het college te kunnen controleren op het gebied van privacybescherming.
- De accountant beschikt met dit verslag over een in onafhankelijkheid en op expertise gebaseerde beoordeling voor de jaarcontrole.
- Dit verslag hoort leidend te zijn bij BRP-, ENSIA-audits of rekenkamertoetsing voor zover de vraag speelt of de gemeente de AVG naleeft. AVG-toetsing door anderen dan de FG brengt extra administratieve lasten met zich mee en strookt niet met de toezichtsystematiek van de AVG.

[7] De indicatoren op uitvoeringsniveau vormen tegelijkertijd de koppeling met het verwerkingsregister waarover de gemeente volgens artikel 30 AVG moet beschikken. Vgl. de afspraken hierover die we in VNG/IBD-verband hebben gemaakt.

Ontwikkellijn bestuurlijk

Speerpunten	Opzet	Bestaan	Werking	Advies
1. Beleid *Visie, missie en aanpak*				(1) Plaats het privacybeleidskader in het licht van duurzaam databeleid. (2) Zet het belang van duurzaam databeleid af tegen andere bestuurlijke thema's. (3) Maak FG-verslagen onderdeel van horizontale verantwoording.
2. Regie en support *Ondersteuning aan proceseigenaren*				(1) Bevorder begrip bij proceseigenaren en waarom zij behoeftesteller zijn. (2) Benadruk de ondersteunende functie van het PIT. (3) Waarborg de kwaliteit en capaciteit van het PIT. (4) Laat proceseigenaren via de concerndirecteur verantwoording afleggen over hun oplossingen.
3. Toezicht *Kwaliteitsbewaking en data-ethiek*				(1) Betrek de FG naar behoren en tijdig bij alle bestuurlijke aangelegenheden die verband houden met verwerking en bescherming van persoonsgegevens. (2) Blijf hem ruimte geven voor uitoefening van taken. (3) Bevorder FG-regio overleg.
4. Werkprogramma *Plan 'Samen op weg naar digitale duurzaamheid'.*				(1) Relateer het werkprogramma voor de middellange termijn aan duurzaam databeleid. (2) Probeer via het jaarplan zoveel mogelijk 'grote slagen' te maken. Bijvoorbeeld: één integrale DPIA op bescherming van personen bij de gemeentelijke aanpak op het gebied van bijstand, schuldenproblematiek en fraudebestrijding. (3) waarborg korte doorlooptijden van DPIA's en implementatie van maatregelen.
5. Privacy by design *Interne activiteiten en gegevensdeling privacyproof*				(1) Zie toe op de implementatie van DPIA-uitkomsten (2) Vraag bij hogere AVG-risicoscoring de FG nadrukkelijk om DPIA-advies.
6. Ketenregie *Uitbestede activiteiten en gegevensdeling privacyproof*				(1) Beperk ketenregie niet tot 'verwerkersovereenkomsten' maar neem ook verantwoordelijkheid bij deelname in samenwerkingsverbanden. (2) Voer ook in samenwerking met ketenpartners duurzaam databeleid. (3) Baseer ketenregie-afspraken op DPIA-uitkomsten en maak afspraken SMART.
7. Verzoeken, klachten en incidenten *Veerkracht en servicegerichtheid*				(1) Bewaak de goede werking van afhandeling van verzoeken, klachten en incidenten. (2) Draag zorg voor goede incident-administratie (niet alleen datalekken). (3) Blijf lering trekken. (4) Betrek de FG waar nodig – met name bij escalatie van klachten.
8. Communicatie en training/opleiding *Cultuur, begrip en draagvlak*				(1) Waarborg dat informatieverstrekking steeds voldoet aan de eisen van art. 13-14 AVG. (2) Blijf sturen op toereikende kennis en het juiste gedrag van medewerkers. (3) Waarborg met name dat personeels-wisselingen niet kunnen leiden tot een 'kennisgat'.
9. Informatie-beveiliging *Beschikbare, betrouw-bare en veilige informatievoorzieningen*				(1) Herijk informatiebeveiligingsmaatregelen aan de hand van DPIA-uitkomsten. (2) Blijf de landelijke afspraken nakomen volgens de Baseline Informatiebeveiliging Overheid (BIO). (3) Blijf oplossingsgericht en kritisch op de administratieve lastendruk.
10. Budget *Algemene financiële middelen voor duurzaam databeleid*				(1) Draag er zorg voor dat in 2021 passend budget is voor kwalitatief goede AVG-beleidsvoering. (2) Geef het budget voor AVG-management / duurzaam databeleid een aparte post op de gemeentebegroting. (4) voorzie in een reserve voor de bekostiging van juridische bijstand bij rechtszaken.

Ontwikkellijn per aandachtsgebied

Aandachtsgebied	Opzet	Bestaan	Werking	Advies
1. Belastingheffing				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
2. Bescherming en opvang, inclusief rechtsbescherming				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
3. Burgerzaken				Er worden al langere tijd strenge eisen gesteld aan BRP en BSN, maar nog niet zozeer vanuit de AVG. Hanteer daarom evengoed een DPIA-aanpak om een beeld te vormen van de passendheid van maatregelen.
4. Cultuur en sport				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig. Mogelijk blijkt de AVG in dit aandachtsgebied minder een rol te spelen.
5. Fraudeonderzoek				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
6. Gemeenteraad				(1) Heb contact met de FG, zowel de proceseigenaar (griffier) als in het kader van raadstoezicht. Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
7. Interne organisatie				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
8. Jeugd en onderwijs				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
9. Lokale economie				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig. Mogelijk blijkt de AVG in dit aandachtsgebied minder een rol te spelen.
10. Milieu en duurzaamheid				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig. Mogelijk blijkt de AVG in dit aandachtsgebied minder een rol te spelen.
11. Wonen, ruimte en bereikbaarheid				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig. Mogelijk blijkt de AVG in dit aandachtsgebied minder een rol te spelen.
12. Veiligheid en openbare orde				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig. Draag zorg voor de audit conform de ministeriële regeling 'periodieke audit politiegegevens' van 26 juni 2019.
13. Werk en inkomen				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
14. Zorg en welzijn				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl

BIJLAGE 7: TOELICHTING GEBRUIKTE AFKORTINGEN EN BEGRIPPEN

In deze bijlage zijn gebruikte afkortingen en begrippen toegelicht. Bij enkele toelichtingen zijn links naar meer informatie opgenomen.

AB: Algemeen Bestuur

AP: Autoriteit Persoonsgegevens. De AP is de toezichthoudende autoriteit, zoals bedoeld in art. 51 lid 1 AVG. De AP houdt onafhankelijk toezicht op het gebruik van persoonsgegevens. De taken van de AP zijn toezicht, advisering, voorlichting, informatieverstrekking en verantwoording, en internationale taken. Voor meer informatie: https://www.autoriteitpersoonsgegevens.nl/ . De AP heeft ook een korte handreiking voor raadsleden gemaakt.

AVG: Algemene Verordening Gegevensbescherming. De AVG is een Europese verordening waarin maatregelen en voorschriften zijn opgenomen die betrekking hebben op de bescherming van de persoonsgegevens in Europa. De AVG trad in 2016 in werking met een overgangsperiode tot 25 mei 2018.

BIG: Baseline Informatiebeveiliging Nederlandse Gemeenten. De BIG gold in de periode 2012 – 2019. Vanaf 2019 is de BIO (zie hierna) van toepassing.

BIO: De Baseline Informatiebeveiliging Overheid (BIO) is sinds 2019 het basisnormenkader voor informatiebeveiliging binnen de overheid (Rijk, gemeenten, provincies, waterschappen).

CERT: Computer Emergency Response Team. De IBD (zie hierna) is de CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten.

CIO: Chief Information Officer. De hoogste verantwoordelijke binnen een organisatie op het gebied van ICT.

CIS: Center for Internet Security. CIS is een non-profit organisatie die wereldwijd erkende ‘best practices’ opstelt voor het beveiligen van IT-systemen en data.

CISO: Chief Information Security Officer. De CISO is verantwoordelijk voor het implementeren van het informatiebeveiligingsbeleid én het toezicht daarop.

CSIRT: Computer Security Incident Response Team. De IBD (zie hierna) is de CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten.

Datalek: De toegang tot of vernietiging, verlies, wijziging of verstrekking van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie.

DB: Dagelijks Bestuur.
DDoS-aanval: Distributed) Denial-of-Service-aanval. Met een DDoS-aanval wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur aangevallen. Het resultaat van deze aanval is dat diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten.

DIV: Documentaire Informatie Voorziening (in spreektaal vaak: het archief)

DOP: Digitaal Ontwikkel Plan.

DPIA: Data Protection Impact Assessment of gegevensbeschermingseffectbeoordeling. Een DPIA is een onderzoek dat de privacyrisico's van een gegevensverwerking in kaart brengt. In de regel dienen DPIA's uitgevoerd te worden wanneer een organisatie een nieuw systeem of proces wil invoeren. De Autoriteit Persoonsgegevens heeft een lijst gepubliceerd van verwerkingen waarvoor een DPIA verplicht is.

DVO: Dienstverleningsovereenkomst.

FG: Functionaris Gegevensbescherming. Organisaties zijn in bepaalde situaties verplicht een functionaris gegevensbescherming (FG) aan te stellen. De FG houdt binnen de organisatie onafhankelijk toezicht op en adviseert over de toepassing en naleving van de AVG.

GAP-analyse: Een onderzoek waarbij getoetst wordt in hoeverre voldaan wordt aan een bepaalde set van eisen. Het verschil tussen de huidige en gewenste situatie is de 'gap'.

GMT: Gemeentelijk Management Team.

GR: Gemeenschappelijke Regeling.

GRC tool: Governance, Risk & Compliance tool. Een GRC-tool is een hulpmiddel voor het beheren van de governance van een organisatie, het beheren van risico's en het naleven van regelgeving.

IBD: Informatiebeveiligingsdienst. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. Voor meer informatie: https://www.informatiebeveiligingsdienst.nl/ en specifiek voor de handreikingen, factsheets, formats en andere hulpmiddelen van de IBD voor gemeenten: Producten Informatiebeveiliging & Privacy - Informatiebeveiligingsdienst

iRvN: ICT Rijk van Nijmegen. iRvN is een module binnen de Modulaire Gemeenschappelijke Regeling Rijk van Nijmegen. Voor meer informatie: https://www.irvn.nl/

ISMS: Information Security Management System is de Engelse term voor het managementsysteem voor informatiebeveiliging. Een ISMS is een geautomatiseerd systeem waarin – volgens de principes van de PDCA-cyclus (zie hierna) - de administratieve organisatie wordt vastgelegd en beheerd.

ISO 27001: Internationale standaard voor het implementeren, onderhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. De BIO (zie hiervoor) is afgeleid van de ISO 27002:2013 norm en verplicht Nederlandse overheden om het managementsysteem in te richten volgens deze norm.

KPI: Kritische Prestatie Indicator. Met kritische prestatie-indicatoren worden de prestaties van organisaties (of teams of medewerkers) gemeten. Op deze manier kan de voortgang van de uitvoering van beleid of van contractuele afspraken meetbaar en concreet gemaakt worden. Op basis van meetresultaten kan vervolgens besloten worden of bijsturing noodzakelijk is.

Logging: Het registreren van uitgevoerde handelingen in een logbestand zodat monitoring en evaluatie plaats kan vinden. Door middel van logging worden gebeurtenissen in systemen vastgelegd. Bijvoorbeeld wie bepaalde gegevens heeft bekeken of heeft aangepast, maar ook pogingen om ongeautoriseerd toegang te krijgen tot systemen (denk aan DDoS aanvallen of ransomware). Ook kunnen door logging datalekken gesignaleerd of juist uitgesloten worden.
MGR: Modulaire Gemeenschappelijke Regeling Rijk van Nijmegen. Voor meer informatie: https://www.regiorvn.nl/ en https://lokaleregelgeving.overheid.nl/CVDR669794/2

MT: Managementteam.

NBA-LIO en NOREA volwassenheidsmodel: model waarmee het volwassenheidsniveau voor informatiebeveiliging kan worden bepaald. Voor meer informatie: zie bijlage 2 of https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

P&C cyclus: Planning & Control cyclus.

PDC: Producten en Diensten Catalogus.

PDCA-cyclus: PDCA staat voor Plan Do Check Act en betreft een structurele, cyclische aanpak die ook de basis is voor informatiebeveiliging en privacybescherming.

Penetratietest (of kortweg pentest): Een onderzoek waarbij ethische hackers proberen de systemen en netwerken van een organisatie binnen te dringen met als doel het identificeren van kwetsbaarheden en het geven van passende adviezen om die kwetsbaarheiden te verkleinen of op te lossen.

PO: Privacy Officer.

Privacy Baseline: Model waarmee het volwassenheidsniveau voor privacybescherming bepaald kan worden. Voor meer informatie: zie bijlage 2 of https://www.cip-overheid.nl/media/1302/20190506-privacy-baseline-v3_2.pdf

Ransomware: Kwaadaardige software die gegevens, of de toegang daartoe, onmogelijk maakt door informatie te versleutelen (encryptie) en losgeld te eisen.

RvN: Rijk van Nijmegen.

SMART: SMART staat voor Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden. Dit is een algemeen gehanteerde norm, waarbij het uitgangspunt is dat aan hoe meer onderdelen wordt voldaan, hoe helderder de informatie is.

- Specifiek: voor maar één uitleg vatbaar
- Meetbaar: er is sprake van een nulmeting én een streven of prognose
- Acceptabel: de uitvoerder heeft de uitvoering geaccepteerd
- Realistisch: de haalbaarheid is op enigerlei wijze onderbouwd en de gemeente heeft invloed op de realisatie
- Tijdgeboden: er is een te volgen tijdpad benoemd

SO: Security Officer.

Suwinet: Een digitale infrastructuur waarmee de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.
Toestemming Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

VNG: Vereniging van Nederlandse Gemeenten. De VNG ondersteunt gemeenten onder meer op het gebied van informatieveiligheid en privacybescherming. Voor gemeenteraden heeft de VNG diverse zogenaamde Raadgevers opgesteld. Op het gebied van informatiebeveiliging en privacybescherming zijn diverse Raadgevers over de informatiesamenleving interessant voor de gemeenteraad.

WDW: Werkorganisatie Druten-Wijchen.

Wbp: Wet bescherming persoonsgegevens. De Wbp gold vanaf 2001 en is inmiddels vervangen door de AVG.

Wmo: Wet maatschappelijke ondersteuning.

BIJLAGE 8: P&C-DOCUMENTEN OVER INFORMATIEBEVEILIGING EN PRIVACYBESCHERMING

In deze bijlage zijn achtereenvolgens selecties van teksten over informatiebeveiliging en privacybescherming opgenomen uit:

- Begroting 2022;
- Adviesbrieven van de auditcommissie bij de begrotingen;
- Zienswijzen bij de begroting van de MGR (iRvN);
- Boardletters 2018 tot en met 2021;
- Jaarstukken 2020;
- Adviesbrieven van de auditcommissie bij de jaarstukken;
- Zienswijzen bij de begroting en jaarstukken van de MGR (iRvN).

Begroting 2022

In de begroting 2022 is op een aantal plaatsen ingegaan op informatiebeveiliging en privacybescherming:

Programma Bestuur en Organisatie

Vanuit het programma 'Open en Weerbaar' investeren we in het verhogen van het bewustzijn van de informatieveiligheid onder onze inwoners, bedrijven en instellingen. In 2022 bieden we inzicht in sensoren in de openbare ruimte en richten we een systeem in voor de ondersteuning van het recht van inzage.

Bij de toelichting op de baten en lasten van het programma Bestuur en Organisatie is onder meer ingegaan op informatiebeveiliging en privacybescherming:

- AVG proof maken van applicaties
  Vanuit wetgeving komen er nieuwe taken naar ons toe. Dat betekent dat de processen en applicaties die ons bij de uitvoering ondersteunen anders moeten worden ingericht en aangepast om aan de Algemene Verordening Gegevensbescherming (AVG) te voldoen. De Autoriteit Persoonsgegevens kan organisaties die niet aan de AVG voldoen een boete opleggen.
- Duurzame borging privacy
  Door veranderende wetgeving zien we een noodzakelijke structurele toename voor de juridische capaciteit op het thema privacy.
- Informatieveiligheid
  Landelijk is de informatieveiligheid steeds vaker in het nieuws; hackers, die systemen platleggen en losgeld eisen om weer bij de systemen te kunnen. Om de risico's te minimaliseren, zetten we extra in op informatieveiligheid. Zo stellen we een security officer aan. Dat is een functionaris die de afdelingen ondersteunt bij het vertalen van het informatiebeveiligingsbeleid naar in de praktijk toepasbare richtlijnen en procedures.

De digitale versie van de begroting is op onderdelen uitgebreider. Zo zijn in die versie in de programma's onder meer links opgenomen naar 'Actuele stukken en links'. In het programma Bestuur en Organisatie zijn niet de links naar het geldende informatiebeveilings- en privacybeschermingsbeleid opgenomen.

Paragraaf Weerstandsvermogen en risicobeheersing

In deze paragraaf is een top 10 met de belangrijkste risico's opgenomen. In de top 10 staat ook databeveiliging (kans dat dit risico optreedt: 50%, maximale bedrag dat het risico tot gevolg kan hebben: € 1 mln). Het risico is als volgt omschreven:

De verdergaande digitale vastlegging van gegevens vraagt er om alert te zijn op de risico's die automatisering met zich meebrengt. Op basis van het vastgestelde Informatieveiligheidsbeleid werken we in 2021 verder aan de realisatie van alle te nemen maatregelen die gesteld worden vanuit de Baseline Informatieveiligheid Gemeenten (BIG[1]). Daarnaast streven we er naar te voldoen aan de AVG Hiertoe is er een Functionaris Gegevensbescherming benoemd en wordt Privacybeleid vastgesteld en uitgevoerd. We zoeken steeds een goede balans tussen de kerntaken van de gemeente en de privacy van de burger. Hierbij streven we naar transparantie over ons handelen en de achtergronden daarvan. Welke risicovolle gebeurtenissen worden zoal onderkend:

- Het ontstaan van schade aan of verstoring van het terrein en de data van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten als gevolg van het feit dat onbevoegden toegang krijgen tot de fysieke of logische omgeving;
- Verlies, schade of diefstal van apparatuur en/of data;
- Het ontstaan van fysieke bedreigingen en gevaren van buitenaf;
- Verlies, schade of diefstal door nalatigheid of opzettelijk misbruik van panden, apparatuur en data in het bezit van de gemeente;
- Externe leverancier voldoet niet aan de contractueel vastgestelde kwaliteits- en veiligheidseisen.

Adviesbrieven auditcommissie bij begrotingen

De auditcommissie stelt jaarlijks onder meer bij de begroting een adviesbrief aan de raad op. Deze brief bevat aandachtspunten voor de raad bij de behandeling van de begroting, en ook concrete adviezen in de richting van het college en de raad. De auditcommissie geeft invulling aan het opdrachtgeverschap van de gemeenteraad aan de accountant. Omdat een specifieke opdracht aan de accountant is sinds 2018 cybersecurity / IT-beheersing, is de auditcommissie ook actief op dit dossier. De auditcommissie voert hierover ook enkele keren per jaar een gesprek met de accountant. Hieronder zijn citaten opgenomen uit de adviesbrieven bij de begrotingen 2020 en 2022 opgenomen over informatiebeveiliging en/of privacybescherming. In de adviesbrief 2021 is de auditcommissie niet ingegaan op aspecten van informatiebeveiliging en/of privacybescherming.

Adviesbrief auditcommissie bij begroting 2020

De paragrafen bieden ook een plek om te rapporteren over de wijze waarop de gemeente invulling geeft aan de nodige verbeteringen in de bedrijfsvoering en in onze governance. Zo zijn er vanuit de boardletter van de accountant, diverse rekenkameronderzoeken en de nota Verbonden Partijen aanbevelingen geformuleerd op het gebied van dossiervorming en dossierbeheer, onze grondportefeuille, databeveiliging en informatievoorziening en archivering. De verbeterpunten zijn nog niet naar behoren opgelost, (…)

[1] Rekenkamer: vanaf 2020 zijn gemeenten verplicht de Baseline Informatiebeveiliging Overheid (BIO) toe te passen, 2019 was het overgangsjaar van de BIG naar de BIO.

Adviesbrief auditcommissie bij Begroting 2022:

Het college benoemt een top 10 van risico's buiten de grondexploitaties om. Daarbij wordt ook databeveiliging genoemd. Cybersecurity is één van de speerpunten van de auditcommissie in deze raadsperiode en de commissie laat zich graag verder informeren over de voortgang van het plan van aanpak inzake cyber security.

Zienswijzen gemeenteraad bij ontwerpbegrotingen MGR (iRvN) 2021 en 2022

Op grond van de Gemeenschappelijke Regeling MGR (artikel 29, lid 5) kan de gemeenteraad zijn zienswijze bij de ontwerpbegroting naar voren brengen. De gemeenteraad heeft de afgelopen jaren steeds gelijktijdig zijn zienswijzen bij de jaarstukken van jaar x-1 en de ontwerpbegroting van jaar x +1 naar voren gebracht. Hierna zijn de zienswijzen van de raad opgenomen bij de ontwerpbegrotingen 2021 en 2022.

Zienswijzen gemeenteraad bij de ontwerpbegroting MGR 2021 (iRvN)

Ten aanzien van de ontwerpbegroting 2021 plaatsen wij ook enkele kanttekeningen:

- Wij zien de oplopende bezuiniging in 2021 wel verwerkt, maar we roepen u op deze bezuiniging ook meerjarig te verwerken;
- We verzoeken de MGR om te onderzoeken of het moderniseren van met name het IT beheer ons via moderne cloudoplossingen regionale schaalvoordelen op kan leveren (ook met het oog op VNG Samen Organiseren en de visie Common Ground);
- U beschrijft uw rol als ICT- en I&A-adviseur. Wij verzoeken u de iRvN-evaluatie hieromtrent af te wachten;
- Tenslotte plaatsen wij de opmerking dat als gevolg van de coronacrisis er vertraging in levering van apparaten kan plaatsvinden, met een onderuitputting van middelen als gevolg. We vinden het reëel dat u de daarop betrekking hebbende investeringen deels meeneemt naar 2021.

Zienswijzen gemeenteraad bij de ontwerpbegroting MGR 2022 (iRvN)

We merken op dat in de begroting 2022-2023 al een doorvertaling te zien is van de nog lopende evaluatie iRvN en de wijze waarop we regionaal daarin samenwerken. Dit vinden wij prematuur. We gaan allereerst in op efficiency en effectiviteit en zullen daarna op de inhoudelijke doelen uit uw begroting ingaan.

Efficiency: Vanaf 2020 hebben we een taakstelling opgelegd van 3x 1% oplopend tot 3%, vergelijkbaar met de efficiency taakstelling van onze eigen organisatie. Deze wordt door iRvN voor 2021 gerealiseerd, via korting op de indexering. Voor 2022 wordt voorgesteld dit te doen door minder inhuur op Servicedesk. Gezien de investering in meer zelfservice en een verbeterde rapportage op het dienstenlandschap, vinden we dit een logisch voorstel. Conform het advies van de Adviesfunctie verzoeken wij u de generieke korting van 1% vanaf 2023 door te voeren conform de BRN-richtlijnen 2022 en deze niet af te laten hangen van de evaluatie.

Effectiviteit: De bij de oprichting van iRvN geformuleerde doelen (de 4K's. Kortweg; minder meerkosten, behoud van kwaliteit, verzorgen van bedrijfscontinuïteit en meer ontwikkelkansen voor medewerkers) zijn tot nu toe niet in indicatoren vertaald. We zien graag dat deze worden ontwikkeld, zodat we hier, samen met de regio, op kunnen sturen. Dit kan een uitwerking zijn van de evaluatie iRvN.

Inhoudelijke doelen: In het verlengde van de wens tot een regionale informatievisie te komen en vooruitlopend op de uitkomsten van de evaluatie iRvN, geven we een aantal aspecten aan die voor ons daarbij van belang zijn:

- Informatieveiligheid
  De boardletter 2020 van de accountant maakt duidelijk dat sturing op IT- beheersing en beperken van de risico's op cybercrime, te maken krijgen met verhoogde normering. Die vraagt een gezamenlijke inspanning, die momenteel wordt vertaald in een groeidocument met een realistische meerjarige planning van de activiteiten voor Nijmegen samen met iRvN. We willen graag weten of dit binnen de bestaande financiële kaders te realiseren blijft.
- Klanttevredenheid
  Bij de metingen van de klanttevredenheid, is de tevredenheid van de Nijmeegse organisatie niet opgenomen in de 0 en 1-meting. De beschrijving in de begroting laat dus met name het beeld zien van de andere regiopartners. Wij zien graag een voorstel met welke indicatoren die tevredenheid zichtbaar te maken is.
- Kwaliteit performance
  In de afsprakenkaders 2021 zijn algemene indicatoren opgenomen, die vooral een beeld van de technische performance geven. Deze raken de bedrijfsvoering, daar wil het bestuur niet op sturen. We denken dat als gevolg van technologische innovaties in de toekomst minder budget nodig is voor beheer. We willen dan ook graag inzicht in deze ontwikkeling en hoe het budget mogelijk ingezet kan worden voor de verhoogde normering op het vlak van informatieveiligheid en privacy.
- Advisering
  U spreekt ambities uit rond advisering. Wij stellen voor de iRvN-evaluatie hieromtrent af te wachten.
- Datasturing
  Onze bestuurlijke verantwoordelijkheid voor (beleidsontwikkeling rond) datagebruik en sturing daarop is groot. Aansluitend bij de ontwikkeling van ons datahuis, is een herverdeling van databeheertaken wellicht nodig. Wij stellen ook hier voor de iRvN-evaluatie af te wachten.
- Landelijke samenwerking
  We zien de meerwaarde van landelijke samenwerking via het programma Samen Organiseren, welke een langjarige inspanning vergt.

Boardletters 2018 tot en met 2021

De gemeenteraad is opdrachtgever van de accountant. Deze opdrachtgeversrol wordt in praktische zin ingevuld door de auditcommissie. Specifiek onderdeel van de opdracht aan de accountant is sinds 2018 de cybersecurity / IT-beheersing. De accountant richt zich in zijn controle, en dus ook bij het thema cybersecurity, primair op de opzet, het bestaan en (waar mogelijk en relevant) de werking van de interne beheersingsmaatregelen, voor zover relevant voor de controle van de jaarrekening. De accountant doet verslag van zijn bevindingen op dit punt in de boardletter.

Uit de samenvatting van de boardletter 2018

- Interne beheersingsomgeving is op orde met uitzondering van de IT-beheersing
- Verbeteringen ten aanzien van de algemene IT beheersmaatregelen in het kader van de controle van de jaarrekening zijn noodzakelijk
- Wij adviseren dringend vanwege het toenemende belang en afhankelijkheid van een veilige en betrouwbare IT-omgeving op basis van een concreet actieplan met o.a. deadlines en het benoemen van een actieverantwoordelijke op korte termijn tot een daadwerkelijke implementatie van de noodzakelijke

verbeteringen ten aanzien van de IT-systemen te komen. (…). Op basis van een dergelijke risicoanalyse en generieke normenkaders maakt u inzichtelijk welke beheersmaatregelen minimaal aanwezig moeten zijn.

Uit de samenvatting van de boardletter 2019

- De interne beheersing kan op onderdelen verder worden versterkt en efficiënter worden ingericht. Eén van de belangrijkste aandachtspunten die wij aan u voorgaand jaar hebben meegegeven is het opvolgen van de IT bevindingen, omdat dit van belang is een volgende stap te kunnen zetten in de doorontwikkeling van de kwaliteit van de interne beheersing. Wij hebben vastgesteld dat hieraan nog geen adequate opvolging is gegeven.
- Wij concluderen dat de gemeente zich bewust is van cyberrisico's. (…). Echter er is nog geen dermate volwassen beleid geïmplementeerd zodat in de volle breedte antwoord gegeven kan worden op cyberrisico's.
- (…). Wij adviseren een inventarisatie te maken van alle kritische onderdelen en periodiek te bekijken of er geen ongeautoriseerde handelingen zijn uitgevoerd met betrekking tot deze kritische onderdelen.

Uit de samenvatting van de boardletter 2020

- Overall beeld is dat de interne beheersing in opzet verder is verbeterd. Het belangrijkste aandachtspunt dat wij voorgaande jaren hebben gerapporteerd is het opvolgen van de IT-audit bevindingen. (…). Het afgelopen jaar heeft uw gemeente in opzet een aantal concreter verbeteringen doorgevoerd in de geautomatiseerde gegevens verwerking, Wij adviseren uw college om het komend jaar prioriteit te geven aan de implementatie van deze ingezette verbeteracties.
- Cybersecurity heeft uw aandacht maar kan verder worden versterkt.
- Wij zien een positieve ontwikkeling op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en adviseren om na te gaan hoe de verbreding naar het informatiebeveiligingsaspect verder vorm kan krijgen.
- De gemeente Nijmegen is één van de eerste gemeenten die in samenwerking met de VNG de SIEM (Security Information & Event Management) implementatie aan het realiseren is. Dit is een positieve ontwikkeling waarbij Nijmegen is aangesloten bij het landelijk initiatief om de technische informatiebeveiliging naar een hoger volwassenheidsniveau te tillen.
- Wij adviseren de beheersing rondom persoonlijke apparaten (zoals laptops, telefoons en tablets) aan te scherpen.
- Opzet algemene IT-heersmaatregelen verbeterd, implementatie nog niet altijd aantoonbaar. (…). Wij adviseren uw college op korte termijn beleid vast te stellen (IT-governance) (…). (…) en vervolgens, als onderdeel van IT-governance, een detailplan op te stellen met o.a. deadlines en het benoemen van een actieverantwoordelijke op te stellen, zodat op korte termijn overgegaan kan worden tot de daadwerkelijke implementatie van de noodzakelijke (resterende) verbeteringen.

Uit de samenvatting van de boardletter 2021

- Ons overall beeld is dat er ruim voldoende aandacht is voor de interne beheersing van processen. Verschillende verbeteracties zijn ingezet om deze interne beheersing verder te versterken. (…). Ondanks deze ingezette verbeteringen laat het onverlet dat een aantal bevindingen uit onze boardletters al meerdere jaren open staat. Voorbeelden hiervan zijn: (…) en het doorontwikkelen en versterken van de IT-omgeving.
- De openstaande observaties zien toe op de implementatie van relevante beheersmaatregelen rondom autorisaties en de rechtenstructuur binnen de applicaties. Dit is de volgende stap in het groeipad tot een volwassen interne beheersing van de IT-omgeving van de gemeente Nijmegen.

- In 2021 heeft de gemeente Nijmegen het informatiebeveiligingsbeleid geactualiseerd. Het aangepaste beleid sluit aan bij de doelstellingen van de gemeente en staat aan de basis van het ambitiedocument 2021-2023 waarin het groeipad van de gemeente is geformuleerd. (…).
- Om het bereiken van de doelstellingen uit de beleidsstukken te kunnen meten is het formuleren van Kritische Prestatie Indicatoren (KPI's) van groot belang. Hoewel uw gemeente een start heeft gemaakt met het formuleren van de KPI is een verdere uitwerking benodigd. (…).
- Daarnaast wijzen wij uw gemeente nogmaals op het belang van het inzichtelijk maken en beheersen van risico's ten aanzien van de samenwerking met leveranciers.
- De verdeling van taken en verantwoordelijkheden tussen uw gemeente en het iRvN, alsmede het afleggen van verantwoording hierover, verdient aandacht.
- Wij adviseren uw gemeente capaciteit vrij te maken om op korte termijn de aanbevelingen uit onze eerdere IT-audits daadwerkelijk te implementeren. Hierbij is het van belang om prioriteiten in de aanbevelingen aan te brengen op basis van het risico-profiel van de data en de systemen, (…).
- Tenslotte zien wij een belangrijke rol voor het college in het bewaken van de voortgang van de doelstellingen zoals deze zijn geformuleerd in het ambitiedocument 2021 – 2023, alsmede het kunnen inspelen op actuele ontwikkelingen op dit gebied.

Jaarstukken

In de jaarstukken 2020[2] is op een aantal plaatsen ingegaan op informatiebeveiliging en privacybescherming. Hieronder is aangegeven waar het concreet om gaat.

Programma Bestuur en Organisatie

We werkten aan onze informatieveiligheid en privacy

Als betrouwbare overheidsorganisatie hebben we doorgewerkt aan de verbetering van ons programma rond informatieveiligheid en privacy. Daarbij zorgden de inbraak bij de Universiteit Maastricht en Citrix crisis er in 2020 voor, dat wij ons meer bewust werden van de kwetsbaarheden rond IT. We hebben samen met iRvN belangrijke stappen gezet die de veiligheid van onze systemen en processen verhogen en die ons reactievermogen zullen verbeteren. We hebben een actieprogramma gestart om de risico's op cybercriminaliteit te monitoren en zullen voortdurend alert zijn op aanvullende maatregelen die we kunnen nemen om extra beveiliging te verbeteren. (…). Ook blijven we actief met acties in het kader van bewustwording op deze thema's. Op het gebied van privacy hebben we ook veel bereikt in 2020. (…). Ook is dit jaar de route vastgesteld hoe elke afdeling de komende jaren verder privacy-proof kan worden gemaakt. (…). Tot slot is in 2020 ingezet op verbeteracties om tot verdere bewustwording te komen. Dit blijft een terugkerend thema komende jaren.

Paragraaf Verbonden partijen (iRvN)

Het jaar voor de iRvN is gekleurd door de Citrix- en corona-crisis. Daarmee is de aandacht voor de risico's van cybercriminaliteit en informatieveiligheid in de spotlight gekomen en in het verlengde daarvan ons bestuurlijk handelen. Voor beide crises bleek de iRvN de zaken op orde te hebben. Samen met de gemeentelijke organisatie zijn waardevolle ervaringen opgehaald voor het aanscherpen van ons basis i-crisisproces en bleken we goed in staat werk vanuit thuis online te kunnen voortzetten. Hierbij was voldoende aandacht voor bewustwording bij medewerkers op hacking en phishing enerzijds en verhoging

[2] Op het moment van afronding van het onderzoek waren de jaarstukken 2021 nog niet beschikbaar.

digitale vaardigheid anderzijds. Daarin heeft iRvN goede service en ondersteuning kunnen bieden. Ten slotte zien we dat de verdergaande digitalisering van onze bedrijfsprocessen tot een wijziging van de ondersteuningsbehoefte leidt. De rol van applicatiebeheer verschuift deels naar leveranciers. Terwijl de komende jaren voor iRvN de realisatie van ons kantoorautomatisering (privacyproof, informatieveilig, archiefwaardig) via de lijn van het landelijke programma Samen Organiseren tot stand gaat komen. Ten slotte zijn we in 2020 gestart met het evaluatie onderzoek (5 jaar werken met iRvN) die in 2021 tot een advies leidt over de doorontwikkeling van iRvN naar de toekomst toe.

Paragraaf Weerstandsvermogen en risicobeheersing

De tekst uit de jaarstukken 2020 is identiek aan die uit de begroting 2020:

De verdergaande digitale vastlegging en verwerking van gegevens vraagt erom alert te zijn op de risico's die automatisering met zich meebrengt. Op basis van het vastgestelde Informatieveiligheidsbeleid werken we in 2021 verder aan de realisatie van alle te nemen maatregelen vanuit de Baseline Informatiebeveiliging Overheid en AVG en werken we volgens een vastgesteld privacybeleid. We zoeken steeds een goede balans tussen de kerntaken van de gemeente en de privacy van burgers. Hierbij streven we naar transparantie over ons handelen en de achtergronden daarvan.

Welke risicovolle gebeurtenissen onderkennen we zoal:

- Het ontstaan van schade aan of verstoring van het terrein en de gebouwen van de gemeente;
- Het beschadigen of verwijderen van data van de organisatie, bedrijfsmiddelen en de onderbreking van de bedrijfsactiviteiten als gevolg van het feit dat onbevoegden toegang krijgen tot de fysieke of logische omgeving;
- Verlies, schade of diefstal van apparatuur met of zonder data;
- Het ontstaan van fysieke bedreigingen en gevaren van buitenaf (natuur);
- Verlies of schade door misbruik van/door medewerkers;
- Een externe leverancier voldoet niet aan de contractueel vastgestelde kwaliteits- en veiligheidseisen.
- De (digitale) data van de gemeente wordt ten onrechte niet of te laat vernietigd. Maar in andere gevallen juist niet lang genoeg bewaard.

Gevolgen:

- Onbevoegde toegang tot kritieke systemen en/of waardevolle data kan leiden tot misbruik van informatie voor fraude of andere criminele activiteiten.
- De gemeente werkt steeds meer samen met ketenpartners en besteedt steeds meer taken uit. Om dit mogelijk te maken delen we (rechtmatig) data. Bij beheer van systemen en gegevens door een derde partij, kunnen door toedoen van deze derde partij, ook data van de gemeente op straat belanden. In andere gevallen kunnen ze door derden onjuist of voor andere doeleinden dan bedoeld of toegestaan gebruikt worden.
- De gemeente voldoet niet aan de aan haar gestelde kwaliteits- en veiligheidseisen als de externe leveranciers zich niet houden aan de contractueel vastgestelde eisen en de gemeente dit niet periodiek of structureel toetst.
- Data die nodig zijn voor verantwoording en geschiedschrijving zijn niet meer beschikbaar.

Maatregelen:

- Toegang tot niet-openbare gedeelten van gebouwen, beveiligingszones, netwerkzones en programmatuur is alleen mogelijk na autorisatie daarvoor.
- In diverse panden (of zones) van de gemeente maken we gebruik van cameratoezicht.
- We beschermen (data)verbindingen tegen interceptie of beschadiging. (…).
- We beveiligen applicatie omgevingen evenals de ondersteunende programmatuur die we gebruiken voor beheer.
- We monitoren, loggen en analyseren activiteiten.

- We verwijderen gegevens en programmatuur van apparatuur of overschrijven deze veilig voordat we de apparatuur afvoeren. (…).
- We bewaren en vernietigen data conform de Archiefwet 1995 en de daaruit voortvloeiende archiefbesluiten en de Algemene verordening gegevensbescherming (AVG).
- We werken structureel aan het bewustzijn van de medewerkers binnen de gemeentelijke organisatie, leveranciers en derden die uitvoering geven aan deel- of ketentaken. (…).
- Bij externe hosting van data en/of services (uitbesteding) blijft de gemeente eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Het voldoen aan de hiervoor geldende regels vereist goede (contractuele) afspraken en controle daarop door middel van contractmanagement.

Adviesbrieven van de auditcommissie bij de jaarstukken

De auditcommissie stelt jaarlijks onder meer bij de jaarstukken een adviesbrief aan de raad op. Deze brief bevat aandachtspunten voor de raad bij de behandeling van de jaarstukken, en ook concrete adviezen in de richting van het college en de raad. De auditcommissie geeft invulling aan het opdrachtgeverschap van de gemeenteraad aan de accountant. Omdat een specifieke opdracht aan de accountant is sinds 2018 cybersecurity / IT-beheersing, is de auditcommissie ook actief op dit dossier. De auditcommissie baseert haar adviesbrief niet alleen op de jaarstukken zelf, maar ook op andere relevantie stukken en gesprekken met betrokkenen. Voor wat betreft het onderwerp informatiebeveiliging en privacybescherming gaat het om:

- de boardletter van de accountant;
- gesprekken met de accountant;
- gesprekken met de portefeuillehouder en sleutelfiguren uit de ambtelijke organisatie.

In de adviesbrief bij de jaarstukken 2020 is de auditcommissie niet specifiek ingegaan op zaken rond informatiebeveiliging en privacybescherming. Naar aanleiding van de jaarstukken 2019 vroeg zij daar wel aandacht voor. Bij die jaarstukken heeft de auditcommissie een initiatiefraadsvoorstel opgesteld in plaats van een adviesbrief. Het initiatiefraadsvoorstel is unaniem aangenomen door de gemeenteraad. Beslispunt 3 is relevant voor dit onderzoek: Het college te verzoeken om met voorrang te sturen op de aandachtspunten ten aanzien van de bedrijfsvoering die de accountant in zijn bevindingen constateert, met name IT-beheersing, dossiervorming en 'softcontrols'.

Jaarstukken MGR (iRvN) 2019 en 2020 en zienswijzen van de raad

Op grond van de Gemeenschappelijke Regeling MGR (artikel 31, lid 3) kan de gemeenteraad zijn zienswijze bij de jaarstukken naar voren brengen. De gemeenteraad heeft de afgelopen jaren gelijktijdig zijn zienswijzen bij de jaarstukken van jaar x-1 en de ontwerpbegroting van jaar x +1 naar voren gebracht. Hierna zijn de zienswijzen van de raad opgenomen bij de jaarstukken 2019 en 2020[3].

[3] Op het moment van afronding van dit onderzoek waren de jaarstukken 2021 nog niet beschikbaar.

Zienswijzen van de gemeenteraad bij de jaarstukken MGR 2019 (module iRvN)

U beschrijft uw inspanningen in 2019 op het gebied van het veilig en effectief beheren, exploiteren en ontwikkelen van de technische ICT-infrastructuur. We zien de resultaten van deze inspanningen terug en we plaatsen ook enkele kanttekeningen:

- We zijn tevreden met de geringe overlast die we in de regio ervaren hebben als gevolg van hacks. Desondanks roepen wij u op om meer aandacht aan dit onderwerp te besteden, bijvoorbeeld in de risicoparagraaf van de begroting;
- We zijn blij met de melding dat iRvN alle verplichte en aanbevolen open standaarden toepast in haar beheer. In de rapportage zien we daarnaast graag overgenomen welke open source applicaties de iRvN in beheer heeft;
- We zijn blij met de inspanningen op het gebied van de bestrijding van cyberrisico's die, zoals recentelijk weer is gebleken, van groot belang zijn. We nodigen u uit om de aanbevelingen uit het Citrix-evaluatieonderzoek waar nodig op te volgen;
- We zijn ten slotte tevreden met de inspanningen die zijn geleverd om onze bewoners inzagerecht te geven en de applicaties AVG-proof te maken. Wij zijn ons bewust van de inspanning die dit vergt en roepen u op om deze inspanningen voort te zetten.

Zienswijzen van de gemeenteraad bij de jaarstukken MGR 2020 (module iRvN)

We zijn tevreden dat de iRvN binnen het budget de beheeractiviteiten heeft gerealiseerd. We geven over een aantal doelen/resultaten de volgende opmerkingen mee:

- Open standaard/open source
  We zijn blij dat u alle verplichte en aanbevolen open standaarden toepast in uw beheer en tevens in uw rapportage laat zien welke open source applicaties u in beheer heeft of ondersteunt.
- Informatieveiligheid
  We zijn tevreden met uw inspanningen op het gebied van veiligheid en bestrijding van cyberrisico's. We verwachten dat we hierop blijvende inspanning moeten realiseren, gezien de dynamische ontwikkeling waarin cybersecurity zich bevindt.
- Landelijke samenwerking
  De samenwerking die u landelijk zoekt voor de realisatie van infrastructurele voorzieningen, vinden we passend bij onze visie en de bijbehorende doelstellingen.

Rekenkamer(commissie)s
Berg en Dal, Beuningen, Nijmegen en Wijchen



RAPPORT GEMEENTE NIJMEGEN

Weten wat je moet weten

Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming

Juli 2022

COLOFON

Dit rapport is op basis van een gezamenlijk onderzoek opgesteld door de rekenkamer(commissie)s van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen naar informatiebeveiliging en privacybescherming. Voor elk van de vier gemeenten die zijn onderzocht is een aparte versie van het rapport opgesteld. Op onderdelen verschillen die versies van elkaar, omdat er behalve veel gezamenlijke bevindingen ook verschillen zijn tussen de gemeenten. Voorliggend rapport betreft het rapport voor de **gemeente Nijmegen**. Elk rapport is te vinden op de website van de betreffende rekenkamer of bij de rekenkamer op te vragen.

Telefoon	**Website**	**E-mail**
Berg en Dal		
06 28 74 38 98	www.bergendal.nl/rekenkamer	griffie@bergendal.nl
Beuningen		
14 024	Gemeente Beuningen / Rekenkamer	
Nijmegen		
024 – 329 23 38	https://www.nijmegen.nl/over-de-gemeente/rekenkamer/onderzoeksrapporten/	rekenkamer@nijmegen.nl
Wijchen		
088 – 432 72 03	www.wijchen.nl	griffie@wijchen.nl

Bij de uitvoering van het onderzoek zijn de rekenkamer(commissie)s ondersteund door onderzoekers van:

- DMC Group (onderdeel informatiebeveiliging): drs. Chris P.J. Deben CISM, ing. Henk Struving CISA CISSP CISM Lead auditor ISO 27001 en Mick Deben BSc CISSP CRISC;
- Legal2Practice (onderdeel privacybescherming): mr. Jean Paul van Schoonhoven BBA CCO SIO FIP CIPM CIPT CIPP/E, Meindert Boon RA CDPP CIPM CIPP/e, Philippe Dauphin MA BCS Data Protection en Wilfred Brom BC;

Bij het opstellen van de rapportage zijn de rekenkamer(commissie)s ondersteund door drs. Etienne Lemmens van Prae Advies & Onderzoek.

AANBEVELINGEN

In dit rapport zijn concrete aanbevelingen voor versterking van informatiebeveiliging en privacybescherming geformuleerd. We benadrukken daarin de noodzaak om de huidige inspanningen te versterken door hier meer systematisch en cyclisch aan te werken. In de kern zijn alle aanbevelingen daarop gericht. In het rapport worden ze nader onderbouwd en toegelicht; hieronder zijn ze allemaal op een rijtje gezet.

De rekenkamers zijn zich ervan bewust dat de aanbevelingen een forse inspanning vergen van de colleges van B&W. Dat neemt niet weg dat ons inziens alle aanbevelingen - in samenhang - moeten worden opgepakt. Waar zaken niet kunnen wachten, manen we tot spoed. Uiteindelijk zijn het raad en college die samen moeten afspreken in welke volgorde en met welk tijdpad aan de slag wordt gegaan.

We bevelen de gemeenteraden aan om hun college het volgende op te dragen:

1. Zorg voor heldere afspraken tussen de gemeenten en iRvN over informatiebeveiliging
2. Overweeg om het pad in te slaan van gezamenlijk informatiebeveiligingsbeleid in de regio
3. Verhelder het beleid voor informatiebeveiliging en privacybescherming
4. Werk zo snel mogelijk de belangrijkste ontbrekende onderdelen van het beleid uit
5. Voer zo snel mogelijk een organisatiebrede risicoanalyse uit
6. Maak risicomanagement tot een continu proces
7. Stel voldoende (financiële) middelen beschikbaar
8. Geef de CISO en FG de beschikking over een eigen budget
9. Leg vast hoe je gaat toetsen en rapporteren
10. Ga KPI’s gebruiken
11. Zet volop en systematisch in op bewustwording
12. Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming *in de gemeente*
13. Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming *in de regio*

We bevelen de gemeenteraden aan om zelf te zorgen voor de volgende zaken:

14. Stel het beleid voor informatiebeveiliging en privacybescherming vast
15. Laat je informeren en ondersteunen
16. Richt je controlerende rol beter in
17. Overweeg de opdracht aan de accountant voor een IT-audit te continueren
18. Overweeg een regionale aanpak

Tot slot: de rekenkamer is een instrument van en voor de gemeenteraad. Kort samengevat komt ons advies aan de raad op het volgende neer: stel bewust de beleidskaders en doelen vast, bewaak dat het college die oppakt, laat je hierover goed en gericht informeren, stel vragen waar nodig, en zoek daarbij zoveel mogelijk samenwerking met de andere raden in de regio.

Inhoudsopgave

AANBEVELINGEN 1
1. INLEIDING 4
1.1 AANLEIDING VOOR HET ONDERZOEK 4
1.2 DOEL- EN VRAAGSTELLING VAN HET ONDERZOEK 4
1.3 AFBAKENING EN SCOPE VAN HET ONDERZOEK 5
1.4 AANPAK VAN HET ONDERZOEK 7
1.5 LEESWIJZER 9
2. LANDELIJKE KADERS (wet- en regelgeving) 11
3. UITKOMSTEN VAN HET ONDERZOEK 14
3.1 BELANGRIJKSTE UITKOMSTEN 14
3.2 WETEN WIE WAT DOET: TAAKAFBAKENING EN AFSPRAKEN GEMEENTEN-IRVN 17
Het formele kader 17
Taakverdeling informatiebeveiliging: de kaders 18
Taakverdeling informatiebeveiliging: de praktijk in onze gemeenten 20
Aanbevelingen 22
3.3 WETEN WAT JE PLAN IS: GEMEENTELIJK BELEID 22
Vereisten aan beleid en uitwerking 22
Informatiebeveiligingsbeleid: de praktijk in onze gemeenten 23
Privacybeleid: de praktijk in onze gemeenten 26
Aanbevelingen 28
3.4 WETEN WELKE RISICO'S JE LOOPT: RISICOMANAGEMENT DOOR DE GEMEENTEN EN IRVN 29
Instrumenten en tools voor risicoanalyses en -management 30
De praktijk in onze gemeenten: risicomanagement informatiebeveiliging 31
De praktijk in onze gemeenten: beheersen van privacyrisico's 33
Aanbevelingen 33
3.5 WETEN WAT HET KOST: INZET VAN MIDDELEN 33
Hoe organiseer je informatiebeveiliging en privacybescherming? 33
Wat is nodig in termen van personeel en middelen? 35
De praktijk in onze gemeenten: personele inzet 36
De praktijk in onze gemeenten: budget 37
Aanbevelingen 38
3.6 WETEN WAAR JE STAAT: TOETSING EN RAPPORTAGE 38
Toetsing en rapportage: hoe het moet 38
De toetsingspraktijk in onze gemeenten 40
Aanbevelingen 42

3.7 WETEN HOE BELANGRIJK HET IS: BEWUSTWORDING 42
Bewustwording: essentieel onderdeel personeelsbeheer 42
De praktijk in onze gemeenten 43
Aanbevelingen 43
3.8 WETEN DAT JE VERANTWOORDELIJK BENT: BESTUURLIJKE VERANTWOORDELIJKHEID EN COMMITMENT 43
Bestuurlijke verantwoordelijkheid vereist 43
De bestuurlijke praktijk in onze gemeenten 44
De bestuurlijke praktijk op regionaal niveau 44
Aanbevelingen 46
3.9 WETEN HOE JE STUURT EN CONTROLEERT: DE ROL VAN DE GEMEENTERAAD 47
Wat is de rol van een gemeenteraad? 47
De praktijk: de rol van de raad en de informatievoorziening 48
Goede voorbeelden elders 50
Aanbevelingen 51
4. REACTIES COLLEGE VAN B&W EN DAGELIJKS BESTUUR MGR 53
Reactie College 53
Reactie Dagelijks Bestuur MGR Rijk van Nijmegen 56
5. NAWOORD REKENKAMER(COMMISSIE)S 59

Bij dit rapport hoort een bijlagenboek met daarin de volgende bijlagen:

- Bijlage 1: Aanpak van het onderzoek: deelvragen en gesprekspartners
- Bijlage 2: Normenkader, inclusief een toelichting op de gehanteerde volwassenheidsmodellen
- Bijlage 3: 10 bestuurlijke principes informatiebeveiliging en VNG-resoluties
- Bijlage 4: Overzicht van verplichte BIO-documenten
- Bijlage 5: Strategische, tactische en operationele kaders uit Basisafspraken gemeenten - iRvN
- Bijlage 6: Voorbeeld verantwoordingsrapportage aan de gemeenteraad
- Bijlage 7: Verklaring van gebruikte begrippen en afkortingen
- Bijlage 8: P&C-documenten over informatiebeveiliging en privacybescherming

De bijlagen 1 tot en met 7 zijn voor alle vier gemeenten identiek. Voor de gemeente Nijmegen is er één extra bijlage (bijlage 8: P&C-documenten over informatiebeveiliging en privacybescherming).

1. INLEIDING

1.1 AANLEIDING VOOR HET ONDERZOEK

Gemeenten doen op grote schaal aan gegevensverwerking en zij verzamelen, beheren en verwerken daarbij niet zelden gevoelige persoonsgegevens. Die verwerking vindt plaats in steeds complexere structuren van (keten-)samenwerking en uitbesteding. Zij moeten daarbij in toenemende mate letten op de informatiebeveiliging en privacybescherming. Wet- en regelgeving en bestuurlijke afspraken[1] – denk aan de AVG (2016), de BIG (2012) en de BIO (2019), maar ook aan VNG-resoluties (2013 en 2021)[2] en de in VNG-verband vastgestelde 10 bestuurlijke principes voor informatiebeveiliging[3] - dwingen gemeenten om hun informatiebeveiliging serieus te nemen. Doordat de (persoons)gegevens en informatieprocessen steeds meer gedigitaliseerd zijn, worden gemeenten ook kwetsbaarder voor cybercriminaliteit, of die nu bedoeld is om bepaalde gegevens te verkrijgen of als afpersingsmiddel. Gemeenten dienen zich daartegen te wapenen, maar slagen daar niet altijd goed in, getuige recente datalekken en veiligheidsincidenten in bijvoorbeeld de gemeenten Hof van Twente en Buren.

De uitdagingen waarmee gemeenten worden geconfronteerd vormden de aanleiding voor de gezamenlijke rekenkamer(commissie)s[4] in de regio Rijk van Nijmegen om de stand van zaken van de informatiebeveiliging en privacybescherming in hun gemeentelijke organisatie te onderzoeken.

1.2 DOEL- EN VRAAGSTELLING VAN HET ONDERZOEK

De rekenkamers willen met dit onderzoek allereerst de gemeenteraden ondersteunen. De gemeenteraad en individuele raadsleden staan op vrij grote afstand van de dagelijkse zorg voor informatiebeveiliging en privacybescherming in de gemeente. Die zorg is de verantwoordelijkheid van het college van B&W. Maar als kadersteller en controleur van het college is de gemeenteraad wel degelijk verantwoordelijk, samen met het college, voor een goede en stabiele dienstverlening aan burgers en bedrijven, voor goed en stabiel bestuur van de gemeente en voor bescherming van de gegevens van burgers. De gemeenteraad moet controleren of de gemeente hierin geen steken laat vallen. Behalve op de vraag wat de colleges aan informatiebeveiliging en privacybescherming doen, richt het onderzoek zich daarom ook welbewust op de gemeenteraden. Die moeten hun kaderstellende en controlerende taak goed (kunnen) vervullen.

[1] Een toelichting op de wet- en regelgeving is opgenomen in hoofdstuk 2. In hoofdstuk 3 wordt op verschillende plekken gerefereerd aan bestuurlijke afspraken.

[2] https://www.informatiebeveiligingsdienst.nl/product/resolutie-informatieveiligheid/

[3] https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

[4] Voor de leesbaarheid verder: de rekenkamers. Het onderzoek is uitgevoerd door de rekenkamers van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen. De andere gemeenten in het Rijk van Nijmegen (Druten, Heumen en Mook en Middelaar) kenden in de onderzoeksperiode geen (functionerende) rekenkamer.

De doelstelling van het onderzoek is daarom tweeledig:

1. Voor de gemeenteraden inzichtelijk maken hoe de informatiebeveiliging en privacybescherming door hun eigen gemeente ervoor staat, en hoe het college daaraan werkt.
2. De gemeenteraden ondersteunen bij de kaderstelling en controle op dit vlak. Een belangrijke voorwaarde daarvoor is de manier waarop het college de raad informeert.

Dat leidt ook tot een dubbele vraagstelling van dit onderzoek:

1. Is de informatiebeveiliging en privacybescherming van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen voldoende op orde, is er voldoende zicht op de risico's en werken de gemeenten op effectieve en efficiënte wijze aan verbetering van de onderdelen die niet voldoende op orde zijn?
2. Hoe kunnen de gemeenteraden de komende jaren hun kaderstellende en controlerende taak op deze thema's goed vervullen?

Om deze vragen te beantwoorden zijn een groot aantal deelvragen geformuleerd (zie bijlage 1). De deelvragen zijn leidend geweest bij de uitvoering van het onderzoek. De deelvragen zijn onderverdeeld in drie delen:

- Onderzoeksdeel A Informatiebeveiliging
- Onderzoeksdeel B Privacybescherming
- Onderzoeksdeel C Kaderstelling en controle door de gemeenteraden.

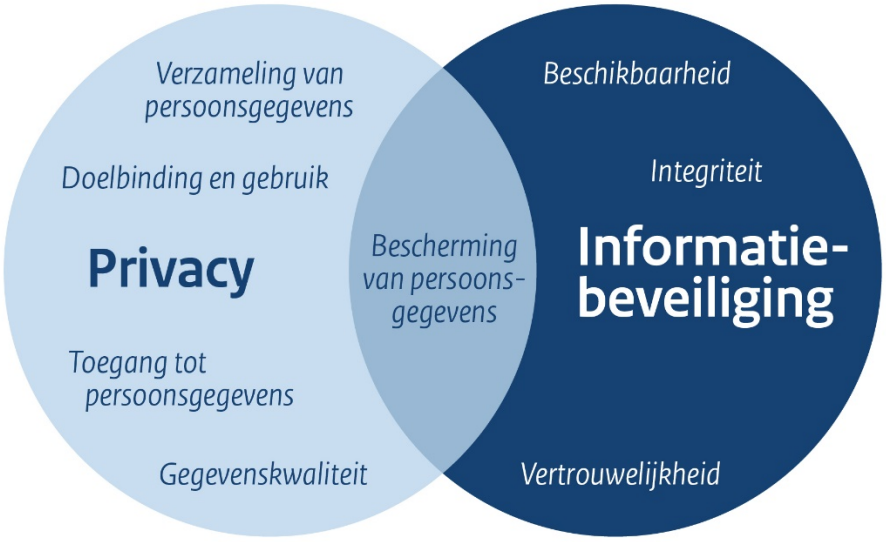
1.3 AFBAKENING EN SCOPE VAN HET ONDERZOEK

Het onderzoek richt zich op informatiebeveiliging en privacybescherming. **Informatiebeveiliging** definiëren wij in het onderzoek als het treffen en onderhouden van een samenhangend pakket maatregelen om de beschikbaarheid, integriteit (juistheid en volledigheid) en vertrouwelijkheid van de (digitale) gegevens in de organisatie te waarborgen. De Cyber Security Alliantie drukt het als volgt uit: informatiebeveiliging is alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. **Privacybescherming** is de toepassing van normen die bepalen hoe persoonsgegevens mogen worden gebruikt. Sommige deskundigen wijzen erop dat de term 'privacy' verwarrend werkt[5], en dat we beter over gegevensbescherming kunnen spreken. Omdat privacybescherming de gebruikelijke benaming is, houden we het in dit rapport daarbij.

Informatiebeveiliging en privacybescherming zijn op diverse manieren met elkaar verbonden. Privacybescherming is niet mogelijk zonder een goede informatiebeveiliging, en diverse (verplichte en aanbevolen) maatregelen die gemeenten nemen – denk bijvoorbeeld aan bewustwording in de organisatie - dragen bij aan zowel informatiebeveiliging als privacybescherming. Figuur 1 laat het verband zien.

[5] https://pmpartners.nl/actueel/laten-we-stoppen-met-privacy/

Figuur 1: Overlap van de terreinen informatiebeveiliging en privacybescherming



Overheden moeten aan allerlei vereisten voldoen op het gebied van informatiebeveiliging en privacybescherming. Daarbij worden vaak de volgende drie zaken onderscheiden:
Opzet: het ontwerp van maatregelen (in beleid, plannen en processen)
Bestaan: dat de maatregelen feitelijk zijn getroffen
Werking: de effectiviteit van de getroffen maatregelen.

Opzet is een essentiële voorwaarde voor goede informatiebeveiliging en privacybescherming. Maatregelen en werkwijzen *kunnen* worden toegepast zonder dat ze schriftelijk zijn vastgelegd. Maar het risico is dan dat er onduidelijkheid ontstaat: wie wat moet doen en op welke wijze. Om die reden is schriftelijke vastlegging en vaststelling zo'n belangrijke en noodzakelijke voorwaarde. In dit onderzoek is vooral gekeken naar de opzet en het bestaan van de maatregelen. Waar mogelijk is ook aandacht besteed aan de werking, in die zin dat we hebben onderzocht of de gemeenten zicht hebben op de werking. De rekenkamers hebben zelf niet de werking c.q. de effectiviteit van het informatiebeveiligings- en privacybeschermingsbeleid onderzocht, bijvoorbeeld door een ethische hacker in te schakelen.

Het onderzoek richt zich op de vier gemeenten waarin onze rekenkamers actief zijn. Zeven gemeenten in het Rijk van Nijmegen (Berg en Dal, Beuningen, Druten, Heumen, Mook en Middelaar, Nijmegen en Wijchen) hebben sinds 2016 hun ICT-taken belegd bij de ICT-module van de Modulaire Gemeenschappelijke Regeling (MGR) Rijk van Nijmegen (iRvN)[6]. Om die reden is ook iRvN in het onderzoek betrokken. Het onderzoek heeft zich met name gericht op de dienstverlening door iRvN aan de vier gemeenten, en niet op de informatiebeveiliging en privacybescherming in de eigen iRvN-organisatie of het openbaar lichaam MGR.

[6] iRvN is de tweede module van de MGR. De eerste module is het Werkbedrijf.

Om het onderzoek uitvoerbaar te houden, is ervoor gekozen om onderzoeksdeel B over privacybescherming voornamelijk te richten op het sociaal domein, in het bijzonder:

- de verwerkingen van persoonsgegevens door gemeenten in het kader van de Jeugdwet;
- het verstrekken van persoonsgegevens:
  - binnen gemeenten aan medewerkers Openbare Orde en Veiligheid;
  - door gemeenten aan samenwerkingsverbanden op het gebied van openbare orde en veiligheid (zoals Veiligheidshuizen en RIEC's[7]).

Een laatste afbakening betreft de onderzochte periode. Het onderzoek in de vier gemeenten en iRvN is uitgevoerd in de maanden juli tot en met oktober 2021. Informatiebeveiliging en privacybescherming zijn terreinen waarop de ontwikkelingen snel gaan, en na afronding van de dataverzameling voor ons onderzoek hebben medewerkers in de onderzochte organisaties natuurlijk niet stilgezeten: al dan niet gestimuleerd door de vragen van de rekenkamers over opzet, bestaan en werking van het informatiebeveiligings- en privacybeschermingsbeleid zijn er sinds oktober 2021 diverse stappen gezet. Wij beschouwen dat als winst: hoe meer voortgang de gemeenten boeken, hoe beter. Hier en daar zijn de uitkomsten van dit onderzoek op het moment van publicatie misschien deels achterhaald. Dat is geen probleem, en wij zien er vooral een aansporing in aan de colleges om de gemeenteraden wat vaker te informeren over de stand van zaken en voortgang op beide terreinen.

1.4 AANPAK VAN HET ONDERZOEK

Bij de uitvoering van het onderzoek zijn de rekenkamers ondersteund door onderzoekers van DMC Group en Legal2Practice. Op basis van het onderzoeksplan zoals vastgesteld en verspreid in juni 2021 is de dataverzameling als volgt aangepakt:

1. Verzamelen en analyseren van documenten en open bronnen onderzoek

Bij de vier gemeenten en iRvN zijn in juli 2021 aan de hand van een vragenlijst documenten opgevraagd. Hen is ook gevraagd eventuele andere relevante documenten binnen hun organisatie, die niet op de lijst zijn opgenomen, te delen. Na ontvangst van de documenten zijn deze aan de hand van de onderzoeksvragen geanalyseerd door de onderzoekers. Parallel daaraan hebben de onderzoekers ook open-bronnenonderzoek uitgevoerd[8]. Dit houdt in dat zij online gezocht hebben naar informatie over en van de vier gemeenten en iRvN, die inzicht kan geven in eventuele risico's, kwetsbaarheden en incidenten die hebben plaatsgevonden.

2. Gesprekken met betrokkenen

Op basis van de bevindingen uit de geanalyseerde documenten en het open-bronnenonderzoek is een groot aantal gesprekken gevoerd met betrokkenen binnen de gemeenten en iRvN. In bijlage 1 is aangegeven met

[7] RIEC: Regionaal Informatie- en Expertise Centrum. De tien RIECs en het LIEC (landelijk Informatie- en Expertisecentrum) ondersteunen partners bij de aanpak van georganiseerde criminaliteit.

[8] In vaktermen: Open Source INTelligence (OSINT).

welke bestuurders en functionarissen is gesproken en waarop de focus lag in het gesprek: informatiebeveiliging (A), privacybescherming (B) of de rol van de gemeenteraden (C).

Omdat het onderzoek zich richtte op vijf verschillende organisaties (vier gemeenten en iRvN) is het een bijzonder arbeidsintensief onderzoeksproces geweest. Daarbinnen bleek het om praktische redenen niet mogelijk om de raadsleden uit onze vier gemeenten te interviewen. Op diverse manieren is echter schriftelijk materiaal verzameld over de manier waarop de gemeenteraden hun rol op de beide beleidsterreinen in de praktijk invullen. Daarnaast is een groepsgesprek gehouden met de vier raadsgriffiers. Onderwerp van gesprek was de wijze waarop de gemeenteraden en -raadsleden in de praktijk hun kaderstellende en controlerende rol invullen.

3. Ordenen onderzoeksmateriaal

Alle verzamelde onderzoeksgegevens zijn door de onderzoekers geordend per organisatie. Daarbij is gebruik gemaakt van zogenaamde 'volwassenheidsmodellen'. Met deze modellen kan bepaald worden wat het volwassenheidsniveau (op een schaal van 1 tot 5) is van de organisatie voor toepassing van de wet- en regelgeving voor informatiebeveiliging en privacybescherming, en hoe groot de risico's zijn die worden gelopen als de wet- en regelgeving (nog) niet (volledig) geïmplementeerd zijn. Voor een uitgebreidere toelichting op deze volwassenheidsmodellen verwijzen wij naar bijlage 2.

4. Bespreking onderzoeksmateriaal met ambtelijke organisatie

De ambtelijke vertegenwoordigers van de gemeenten en iRvN hebben in februari-maart 2022 een mondelinge en schriftelijke reactie gegeven op het ruwe onderzoeksmateriaal van de onderzoekers. Gezien de (veiligheids)risico's van onderzoek naar informatiebeveiliging, en gezien de omvang en het technische karakter van dit onderzoek naar vier gemeenten en iRvN, hebben de rekenkamers besloten om de ambtelijke reacties niet schriftelijk te verwerken in het onderzoeksmateriaal en om geen bevindingenrapport te publiceren.

5. Expertmeeting

In maart 2022 hebben de rekenkamers een digitale expertmeeting belegd met zeven deskundigen op de onderzochte terreinen. De bijeenkomst was met name bedoeld om invulling te geven aan onderzoeksdeel C over de rol van de gemeenteraad. De deskundigen hebben hun ervaringen met het informeren van gemeenteraden (en andere volksvertegenwoordigers) over informatiebeveiliging en privacybescherming met de rekenkamers gedeeld.

6. Opstellen bestuurlijke rapportage

Op basis van het onderzoeksmateriaal, de ambtelijke reacties en de expertmeeting hebben de rekenkamers het voorliggende bestuurlijk rapport opgesteld.

7. Aanbieding voor bestuurlijke reactie

De rekenkamers hebben de colleges en het Dagelijks Bestuur (DB) van iRvN van 20 mei tot en met 28 juni 2022 in de gelegenheid gesteld een reactie te geven op het rapport, in het bijzonder op de aanbevelingen. Die

periode is langer dan gebruikelijk. Na een verzoek van het regionale portefeuillehoudersoverleg, hebben wij ervoor gekozen de gebruikelijke termijn van drie weken met ruim twee weken te verlengen. De colleges en het DB hebben hiervan gebruik gemaakt. De reacties van de colleges zijn door de rekenkamer(commissie)s voorzien van een nawoord.

Hobbels in het onderzoek

Het gezamenlijke rekenkameronderzoek in de vier gemeenten heeft al met al iets minder dan een jaar geduurd. Voor een gemiddeld rekenkameronderzoek is dat een acceptabele duur, maar het is langer dan gepland. De rekenkamers zijn op een aantal hobbels gestuit, die hieronder kort worden beschreven.

Twee onderzoeksterreinen

Een onderzoek op twee verwante maar desondanks aparte beleidsterreinen betekende in de praktijk aanzienlijk grotere onderzoeksinspanningen dan verwacht, ook voor de medewerkers in onze gemeenten. De grote hoeveelheid gevoerde gesprekken (inclusief verslaglegging) betekende een enorme logistieke operatie. Dat werd nog versterkt door de grote hoeveelheid schriftelijke documentatie waarmee onderzoek op deze terreinen gepaard gaat, meer dan in een gemiddeld rekenkameronderzoek.

Documentenuitvraag

De aangeleverde documentatie in de startfase van het onderzoek bleek in de loop van het onderzoek verre van volledig te zijn geweest. Voor zover de rekenkamers het kunnen overzien, had dit deels te maken met het feit dat betrokken medewerkers van zowel gemeenten als iRvN hebben gehandeld als in een audit: zij hebben slechts de in de uitvraag gespecificeerde documenten aangeleverd, ondanks het verzoek van de rekenkamers om 'alle relevante documentatie' aan te leveren. Dit verzoek was, zoals gebruikelijk in rekenkameronderzoek, expliciet opgenomen in de documentenuitvraag, en is ook in diverse gesprekken herhaald. Deze onvolledige aanlevering heeft in een latere fase van het onderzoek veel extra tijd en energie gekost van de onderzoekers en de betreffende medewerkers. We voegen er nog aan toe dat de gebrekkige aanlevering van documentatie ook het gevolg is van het feit dat de gemeenten en iRvN de (verplichte) documentatie niet altijd goed op orde hebben. Dit is een bevinding, waar elders in dit rapport aandacht aan zal worden besteed.

Complexiteit

Het technische, gespecialiseerde en met jargon doordrenkte karakter van met name het terrein informatiebeveiliging betekende dat de rekenkamers meer tijd dan verwacht nodig hadden voor het opstellen van een goed leesbare bestuurlijke rapportage. Die is immers in eerste instantie bedoeld voor de gemeenteraden en colleges, die geen specialisten zijn, maar die de conclusies en aanbevelingen wel moeten kunnen doorgronden en opvolgen.

1.5 LEESWIJZER

In het vervolg van dit rapport geven we in hoofdstuk 2 een toelichting op de landelijke kaders voor informatiebeveiliging en privacybescherming. In hoofdstuk 3 beschrijven we de uitkomsten van het onderzoek aan de hand van een aantal centrale thema's uit het onderzoek. Elk thema sluit af met enkele aanbevelingen.

Deze aanbevelingen zijn vooraan in het rapport op een rij gezet. Voorafgaand aan de thema-beschrijvingen formuleren we in hoofdstuk 3 de belangrijkste uitkomsten uit het onderzoek.

Voorliggend rapport betreft de gemeente Nijmegen. Voor elk van de vier gemeenten die zijn onderzocht is een aparte versie opgesteld. Op onderdelen verschillen die versies van elkaar, omdat er behalve veel gezamenlijke bevindingen ook verschillen zijn tussen de gemeenten.

In hoofdstuk 4 staat de reactie van het college en het DB van de MGR op het rapport, in het bijzonder de aanbevelingen. Het nawoord van de rekenkamer(commissie)s naar aanleiding daarvan is te lezen in hoofdstuk 5.

Bij dit rapport hoort een bijlagenboek. In de bijlagen zijn nadere toelichtingen en meer gedetailleerde informatie opgenomen:

- Bijlage 1: Aanpak van het onderzoek: deelvragen en gesprekspartners
- Bijlage 2: Normenkader, inclusief een toelichting op de gehanteerde volwassenheidsmodellen
- Bijlage 3: 10 bestuurlijke principes informatiebeveiliging en VNG-resoluties
- Bijlage 4: Overzicht van verplichte BIO-documenten
- Bijlage 5: Strategische, tactische en operationele kaders uit Basisafspraken gemeenten - iRvN
- Bijlage 6: Voorbeeld verantwoordingsrapportage aan de gemeenteraad
- Bijlage 7: Verklaring van gebruikte begrippen en afkortingen
- Bijlage 8: P&C-documenten over informatiebeveiliging en privacybescherming

De bijlagen 1 tot en met 7 zijn voor alle vier gemeenten identiek. Voor de gemeente Nijmegen is er één extra bijlage (bijlage 8: P&C-documenten over informatiebeveiliging en privacybescherming).

2. LANDELIJKE KADERS (wet- en regelgeving)

Het belang van een goede informatiebeveiliging en privacybescherming voor gemeenten wordt weerspiegeld in de landelijke wet- en regelgeving. Welke kaders zijn relevant?

Een goede **informatiebeveiliging** vereist het nemen van passende maatregelen door een organisatie. Wat precies 'passende maatregelen' zijn is voor elke organisatie verschillend. Binnen de Nederlandse overheid is afgesproken om vanaf 1 januari 2019 de Baseline Informatiebeveiliging Overheid (BIO) te hanteren als basisnormenkader voor de beveiliging van informatie(systemen). De BIO vervangt de baselines informatieveiligheid die tot dan toe door de verschillende overheidslagen werden gehanteerd; voor gemeenten was dat sinds 2012 de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Afgesproken is dat alle overheidslagen 2019 als overgangsjaar zouden gebruiken voor de implementatie van de BIO en dat ze deze vanaf 1 januari 2020 verplicht hanteren.

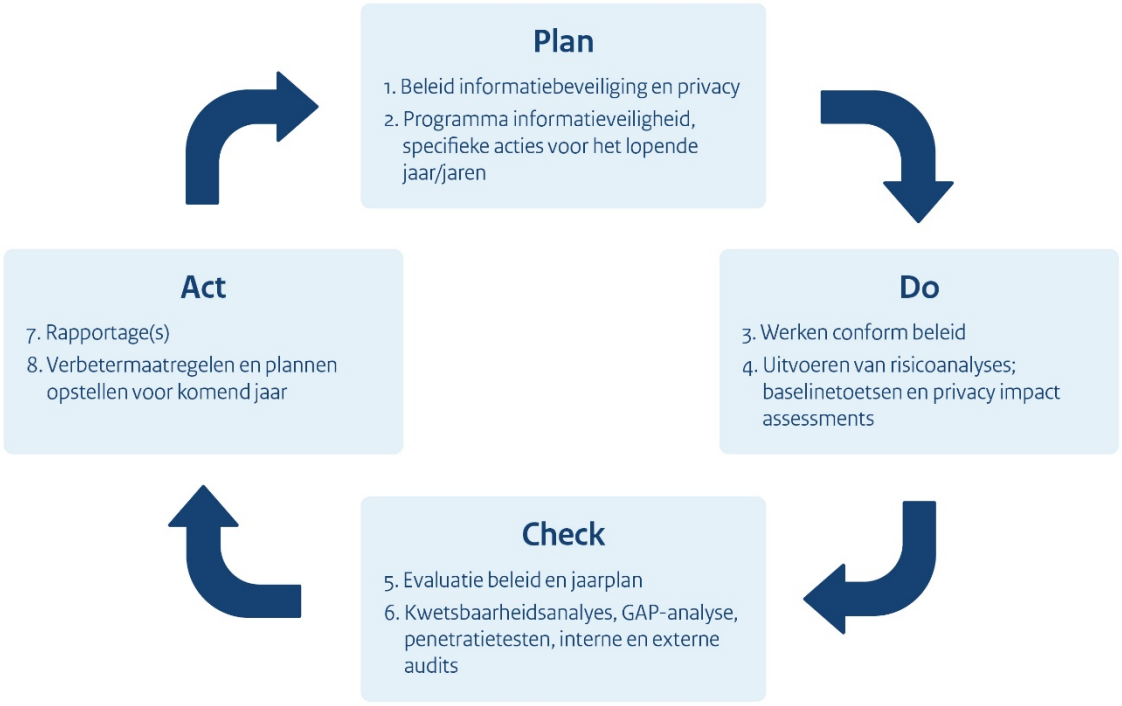
Met de BIO is er één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging[9]. Daarin staat een aantal uitgangspunten en principes centraal:

- Risicomanagement
  Nul risico bestaat niet op het gebied van informatiebeveiliging. Dat betekent dat (bestuurlijk) bepaald moet worden hoeveel en/of welke risico's acceptabel worden gevonden. Omdat dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert, veranderen risico's ook. Er moet daarom continu identificatie en beoordeling van risico's plaatsvinden om te bepalen wat nodig is om informatie adequaat te beschermen.
- Procesmatige aanpak
  Dit betreft feitelijk een vertaling van de PDCA-cyclus (zie figuur 2 op de volgende bladzijde):
  - Vaststellen van beleid en doelstellingen;
  - Implementeren en uitvoeren van operationele maatregelen;
  - Bewaken en controleren van efficiency en effectiviteit van de maatregelen;
  - Continu doorvoeren van verbeteringen.
- Beveiligingsprincipes
  Alle beveiligingsmaatregelen, mechanismen en controles worden geïmplementeerd om invulling te geven aan een of meer van de fundamentele beveiligingsprincipes beschikbaarheid, integriteit en vertrouwelijkheid:
  - Beschikbaarheid: bij beschikbaarheid gaat het om de tijdigheid, continuïteit en robuustheid van data. De data moeten beschikbaar zijn voor gebruikers op het moment dat zij deze nodig hebben.
  - Integriteit: integriteit gaat over de mate waarin informatie juist en volledig is. Elke ongeautoriseerde verandering van data (zowel opzettelijk als per ongeluk) brengt de integriteit van de data in gevaar.

[9] Internationale standaard voor informatiebeveiliging: NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. Deze geven richtlijnen om zeker te stellen dat wordt voldaan aan specifieke beveiligingsdoelstellingen van een organisatie. In de BIO zijn deze richtlijnen uitgewerkt voor de overheid.

- Vertrouwelijkheid: vertrouwelijkheid wordt ook wel exclusiviteit genoemd. Wie kan bij welke informatie? Vertrouwelijkheid heeft te maken met alle maatregelen die ervoor zorgen dat het noodzakelijke niveau van geheimhouding binnen een organisatie geborgd wordt.

Figuur 2: Plan-Do-Check-Act (PDCA)-cyclus voor informatiebeveiliging en privacybescherming



Voor **privacybescherming** liggen de vereisten voor gemeenten vast in de Algemene Verordening Gegevensbescherming (AVG), die in 2016 in werking trad maar een tweejarige overgangsperiode bood tot 25 mei 2018[10]. De AVG is een Europese verordening waarin maatregelen en voorschriften zijn opgenomen die betrekking hebben op de bescherming van de persoonsgegevens in Europa[11]. De meeste bepalingen van de AVG waren voor de Nederlandse overheid niet nieuw: de AVG borduurt voort op veel principes die al te vinden waren in de Wet bescherming persoonsgegevens (Wbp) uit 2001.

De AVG bevat de belangrijkste regels voor de omgang met persoonsgegevens door overheden[12]. Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet en met een gerechtvaardigd doel. Bij het verwerken van persoonsgegevens moet een aantal uitgangspunten in acht

[10] Hier hoort bij de UAVG (Uitvoeringswet Algemene Verordening Gegevensverwerking) die in Nederland uitvoering geeft aan de AVG en de regels eruit verder uitwerkt.

[11] Feitelijk betreft het de EER-landen: de EU-landen plus Liechtenstein, Noorwegen en IJsland.

[12] De AVG geldt ook voor bedrijven en andere organisaties, maar we beperken ons in dit rapport tot (gemeentelijke) overheden.

worden genomen. Zo moeten overheden zo min mogelijk gegevens verwerken en dat binnen een passend beveiligingsregime doen. Het gemeentelijk beleid moet in overeenstemming zijn met de vereisten uit de AVG. Overheidsorganen moeten een interne toezichthouder hebben. Dit is de functionaris gegevensbescherming (FG). Ook is er een externe toezichthouder. In Nederland is dat de Autoriteit Persoonsgegevens (AP). Als een gemeente (of andere organisatie) in gebreke blijft, loopt deze het risico op forse boetes.

De AVG is de belangrijkste basiswet voor de bescherming van persoonsgegevens[13]. Daarnaast gelden er in het sociaal domein specifieke wetten zoals de Jeugdwet, de Wet maatschappelijke ondersteuning (Wmo), de Participatiewet, de Wet gemeentelijke schuldhulpverlening, etc. Deze wetten bevatten op sommige onderdelen specifieke regels die voorgaan op de AVG. Een voorbeeld: de AVG bepaalt dat gegevens niet langer dan noodzakelijk bewaard dienen te worden om het doel waarvoor ze worden verwerkt te bereiken; maar artikel 5.3.4, lid 1 van de Wmo geeft aan dat gemeenten persoonsgegevens 15 jaar moeten bewaren. De AVG regelt de algemene beginselen voor de materiële toepassing maar dient bovenal als raamwerk voor het op te stellen privacyrisicobeheersingsraamwerk (Privacy Control Risk Framework, PCRF). De verplichting voor de colleges van burgemeester en wethouders om een PCRF te hebben ingericht vloeit voort uit art. 5 lid 2 in samenhang met art. 24 lid 1 AVG. Verwerkingsverantwoordelijken zoals in onderhavig onderzoek, de colleges van burgemeester en wethouders, dienen bij de toepassing van het PCRF een Plan-Do-Check-Act (PDCA)-cyclus te doorlopen. Tot slot zijn voor het onderzoek ook enkele specifieke landelijke handreikingen, onder meer van de VNG, meegenomen. In bijlage 2 is het volledige normenkader weergegeven.

[13] Een uitzondering betreft de verwerking van politiegegevens door bijzondere opsporingsambtenaren (boa's). Sinds 2019 valt dit niet meer onder de AVG, maar onder de Wet politiegegevens.

3. UITKOMSTEN VAN HET ONDERZOEK

In dit hoofdstuk behandelen we een aantal centrale thema's in het onderzoek. Het gaat om:

- Taakafbakening en afspraken gemeenten en iRvN
- Gemeentelijk beleid en de nadere uitwerking
- Risicomanagement
- Middelen: budget en personeel
- Toetsing en rapportage
- Bewustwording
- Bestuurlijke verantwoordelijkheid en commitment
- Rol van de gemeenteraad.

Voordat we hierop ingaan, formuleren we de belangrijkste uitkomsten van het onderzoek.

3.1 BELANGRIJKSTE UITKOMSTEN

De rekenkamers hebben in het onderzoek vastgesteld dat de gemeenten en iRvN hard werken aan informatiebeveiliging en privacybescherming, maar ook dat er nog veel moet gebeuren om van voldoende beheersing te kunnen spreken. Dat betekent dat de gemeenten kwetsbaar zijn. Ze lopen niet alleen het risico dat veel extra inspanningen en geld nodig zijn als er problemen ontstaan, maar ook dat de dienstverlening aan inwoners en bedrijven wordt gehinderd of zelfs onderbroken, en dat de belangen van inwoners en ondernemers worden geschaad. Wanneer dergelijke risico's zich daadwerkelijk voordoen, kunnen deze weer leiden tot het dalen van het vertrouwen in de overheid en tot bestuurlijke of reputatieschade. We willen benadrukken dat de gemeentelijke overheid verantwoordelijk is voor het behartigen en beschermen van die belangen.

Op allerlei onderdelen boeken de gemeenten voortgang op deze beide relatief nieuwe beleidsterreinen. We schrijven nadrukkelijk 'relatief' nieuw, want gemeenten moeten al enkele jaren voldoen aan belangrijke wetgeving (AVG en voorlopers) en bindende afspraken tussen overheden (BIO en daarvoor de BIG). De gemeenten richten zich op alle aandachtsgebieden van de BIO en de AVG, en spannen zich in om de personele inzet op deze terreinen op peil te brengen en te houden. Ook wordt er in alle gemeenten gewerkt aan bewustwording van de risico's en de eigen verantwoordelijkheid van medewerkers. Dat is ook nodig, want de IBD[14] waarschuwt niet voor niets in het meest recente Dreigingsbeeld dat de interne, onbedoelde handelingen de belangrijkste bedreiging vormen[15].

Al met al zijn die inspanningen nog niet genoeg om volledig en aantoonbaar aan de normen op beide terreinen te voldoen. Op basis van het onderzoek maken de onderzoekers de inschatting dat de gemeenten

[14] IBD: InformatieBeveiligingsDienst. De IBD is onderdeel van de Vereniging Nederlandse Gemeenten (VNG) en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacybescherming.

[15] Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2021/2022 van de IBD.

zich ergens tussen volwassenheidsniveau 1,5 en 2[16] bevinden, zowel voor informatiebeveiliging als voor privacybescherming. Alleen voor Nijmegen schatten de onderzoekers het volwassenheidsniveau voor privacybescherming hoger: tussen de 2 en 3. Zoals aangegeven is voor iRvN alleen een inschatting gemaakt van het volwassenheidsniveau voor informatiebeveiliging. Dit ligt rond niveau 2. Deze schattingen zijn gebaseerd op een totaaloordeel over alle 15 aandachtsgebieden van het NBA-LIO[17] en NOREA-volwassenheidsmodel (voor informatiebeveiliging) en alle 13 thema's uit de Privacy Baseline van het Centrum Informatiebeveiliging en Privacybescherming (voor privacybescherming). Om volledig en aantoonbaar in control te zijn, moeten de organisaties over de volle breedte minimaal op volwassenheidsniveau 3 zitten. Dat is voor geen van de gemeenten aan de orde. Overigens geldt voor de meeste gemeenten in Nederland dat ze nog niet op volwassenheidsniveau 3 (of hoger) zitten.

In het onderzoek hebben we gewerkt met beoordelingsnormen die aansluiten bij de landelijke kaders. Een cruciaal onderdeel hiervan is dat je als organisatie de landelijke kaders hebt vertaald naar gemeentelijk beleid, en dat je het beleid en belangrijke processen op papier hebt vastgelegd en vastgesteld, up to date houdt en aantoonbaar uitvoert en monitort. Op dit punt zien we dat er nog veel te verbeteren is in onze gemeenten. Dat is een belangrijke verklaring voor de te lage volwassenheidsniveaus. Is het reëel om gemeenten, en zeker kleinere gemeenten, aan die norm te toetsen? Het antwoord daarop is een volmondig 'ja'. Gemeenten moeten immers aan de wettelijke normen en bestuurlijke afspraken voldoen. Maar misschien nog wel belangrijker: het is in het belang van hun inwoners. Zo hebben de bestuurslagen met elkaar afgesproken dat elke overheid de ongeveer 60 op grond van de BIO noodzakelijke documenten zodanig op orde moet hebben dat de actuele, vastgestelde versies bij wijze van spreken zo uit de kast zijn te trekken. Dat is dus het minste dat wij mogen vragen. Goed gedocumenteerde en vastgestelde processen zijn een voorwaarde voor een goede uitvoering, zowel door de gemeenten als door hun samenwerkingsorganisatie iRvN. Dit vraagt veel menskracht (kwantitatief en kwalitatief) en geld, en die zijn voor elk van onze gemeenten niet onbeperkt. Maar het is een noodzakelijke investering, want als het niet gebeurt is de gemeente kwetsbaar.

Het organiseren van informatiebeveiliging en privacybescherming moet in organisaties verlopen via de Plan-Do-Check-Act-cyclus[18]. Die PDCA-cyclus is geen onnodig managementjargon, maar een essentiële cyclus die elke organisatie voortdurend moet doorlopen: van beleid, uitvoeringsplannen en concrete maatregelen (Plan), via implementatie en uitvoering (Do), naar toetsen en evalueren (Check) en uiteindelijk verantwoorden en bijsturen (Act). Het onderzoek laat zien dat de gemeenten dit niet goed genoeg doen.

De eerste stappen in de cyclus worden wel gezet. Er is overkoepelend beleid op beide terreinen, maar goed uitgewerkte uitvoeringsplannen en jaarplannen ontbreken veelal. Op diverse onderdelen is het overkoepelend

[16] Volwassenheidsniveau 1: ad-hoc. Volwassenheidsniveau 2: beheerst. Volwassenheidsniveau 3: vastgesteld. Een uitgebreidere beschrijving van de volwassenheidsniveaus is opgenomen in bijlage 2.

[17] NBA-LIO: Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) - Ledengroep Intern en Overheidsaccountants (LIO).

[18] Zie hoofdstuk 2 voor een visualisatie en toelichting.

beleid nader uitgewerkt in de vereiste onderwerpspecifieke beleidsdocumenten op tactisch niveau, maar op veel onderdelen ontbreekt die tactische uitwerking, wat weer onvoldoende basis biedt voor werkinstructies op operationeel niveau. De gemeenten kunnen de vereiste 60 documenten niet allemaal aanleveren. Een voorbeeld is dat geen van de gemeenten vastgesteld beleid heeft voor logging[19] en geen van de gemeenten opdracht aan iRvN heeft gegeven voor het controleren van logging van applicaties. Dat is een belangrijk gemis – en daarmee een risico - in het beveiligingsbeleid van de gemeenten. In de uitvoering gebeurt overigens van alles: soms op basis van uitgewerkte plannen en maatregelen (Plan), maar vaak ook zonder dat die documenten er zijn (Do). In alle gemeenten wordt onvoldoende getest, vastgelegd en geëvalueerd (Check) en daarmee ook onvoldoende bijgestuurd (Act). De cyclus wordt dus niet afgemaakt en herhaald. Daarmee maken de gemeenten zich kwetsbaar.

In onze gemeenten en binnen iRvN zijn de professionals zich zeer bewust van deze kwetsbaarheid. De colleges zijn zich hier ook van bewust, maar kunnen en moeten meer doen om de risico's te verminderen. Hun rol is cruciaal: informatiebeveiliging en privacybescherming zijn 'Chefsache', zou je à la Angela Merkel kunnen zeggen[20]. Als zij het belang voortdurend benadrukken, ruimte scheppen en rugdekking bieden aan de medewerkers die ermee bezig zijn, dan maakt dat verschil. De VNG heeft daartoe 10 cruciale bestuurlijke principes voor informatiebeveiliging geformuleerd. Die principes zijn in onze gemeenten in het beleid opgenomen, maar de meeste bestuurders geven aan de principes in de praktijk niet te hanteren.

In de dagelijkse aansturing in de eigen gemeente zien we dit ook terug in de gang van zaken: er worden weinig besluiten genomen over essentiële zaken als volwassen risicomanagement en de prioritering van risico's, over concrete doelen en ambities en wat daarvoor (minimaal) nodig is in termen van capaciteit, en er is niet of nauwelijks aandacht voor het toetsen, controleren en evalueren, om te weten hoe je er als gemeente voor staat. In het verlengde hiervan is in MGR-verband de bestuurlijke aandacht voor iRvN beperkt en wordt informatiebeveiliging door de bestuurders als 'bedrijfsvoering' afgedaan. Dat leidt ertoe dat de aansturing (governance) van iRvN ambtelijk wordt opgepakt, vaak zonder dat belangrijke keuzes en afwegingen bestuurlijk worden besproken en vastgesteld. Bestuurders doen er niet alles aan om iRvN in positie te brengen: omdat iRvN niet is ingericht als één gezamenlijke informatiedienst met gemeenschappelijk beleid voor informatiebeveiliging, zijn het dus de gemeenten die iRvN moeten voorzien van beleid op alle belangrijke aandachtsgebieden. Het deels ontbreken daarvan is geen issue op bestuurlijk niveau, zo hebben de rekenkamers vastgesteld.

Op relatief grote afstand van deze dagelijkse gang van zaken staan de gemeenteraden. Dat is niet persé erg, maar de raad moet wel zijn verantwoordelijkheid kunnen waarmaken: als gegevens van inwoners niet veilig zijn en dienstverlening op enig moment in gevaar zou komen, is de gemeenteraad daarop aanspreekbaar. Raadsleden moeten hun controlerende taak kunnen waarmaken. Dat gebeurt nu echt onvoldoende. Onze

[19] Door middel van logging worden gebeurtenissen in systemen vastgelegd. Bijvoorbeeld wie bepaalde gegevens heeft bekeken of heeft aangepast, maar ook pogingen om ongeautoriseerd toegang te krijgen tot systemen (denk aan DDOS aanvullen of ransomware). Ook kunnen door logging datalekken gesignaleerd of juist uitgesloten worden.

[20] Zie ook principe 4 van de 10 bestuurlijke principes die de VNG in aanvulling op de BIO heeft geformuleerd.

gemeenteraden weten in het algemeen (te) weinig van de staat van de informatiebeveiliging en privacybescherming in hun gemeente. Er zijn lichte verschillen tussen de gemeenten en in elke raad zijn enkele raadsleden die er meer belangstelling voor hebben. Maar de raad als geheel is in geen van onze gemeenten goed in staat om te controleren of de beheersing voldoende is, ook omdat de informatievoorziening vanuit het college daarvoor niet geschikt is. Het is een taak van het college om de raad goed te informeren over de stand van zaken en de risico's die de gemeente loopt, zo nodig in beslotenheid. Vandaar ook de titel van dit rapport: 'Weten wat je moet weten'. Dat is geen sinecure, op complexe beleidsterreinen met veel jargon, waar de meeste bestuurders ook niet in zijn gespecialiseerd. Maar het moet en kan echt beter dan nu gebeurt.

3.2 WETEN WIE WAT DOET: TAAKAFBAKENING EN AFSPRAKEN GEMEENTEN-IRVN

Een belangrijke vraag in het onderzoek is hoe de taken en verantwoordelijkheden op het gebied van informatiebeveiliging tussen de vier gemeenten en iRvN zijn verdeeld. iRvN voert voor de gemeenten ICT-taken uit, en dat roept de vraag op of iRvN ook verantwoordelijk is voor (een deel van) de informatiebeveiliging. Voor privacybescherming geldt deze vraag niet: iRvN is een verwerker van gegevens van de gemeenten, waarmee ook een verwerkersovereenkomst is gesloten. Deze rol van iRvN is in het onderzoek niet meegenomen.

Het formele kader

De gemeenten in het Rijk van Nijmegen (Berg en Dal, Beuningen, Druten, Heumen, Mook en Middelaar, Nijmegen en Wijchen) hebben hun ICT-taken belegd bij ICT Rijk van Nijmegen (iRvN)[21], de tweede module van de Modulaire Gemeenschappelijke Regeling (MGR) Rijk van Nijmegen. Met uitzondering van de gemeente Wijchen namen alle gemeenten vanaf de start op 1 januari 2016 deel aan de module ICT. Vanaf 1 januari 2018 voert iRvN ook de ICT-taken voor de gemeente Wijchen uit. Dit is pas geformaliseerd met de publicatie van de aangepaste Gemeenschappelijke Regeling (GR) op 1 januari 2022[22].
Aan de module ICT is "de taak opgedragen de continuïteit en kwalitatief adequate dienstverlening op het gehele terrein van de ICT-infrastructuur en –voorzieningen van alle deelnemende gemeenten te verwezenlijken" [23]. Dit houdt in dat iRvN de dagelijkse bedrijfsvoering van de deelnemende gemeenten nu en in de toekomst mogelijk maakt door het neerzetten, onderhouden en ontwikkelen van de benodigde

[21] Behalve de ICT-taken van de gemeenten zijn ook de ICT-taken van de Omgevingsdienst Regio Nijmegen (ODRN) bij iRvN belegd. Deze maakte geen onderdeel uit van het onderzoek. Voor de leesbaarheid noemen wij deze ook niet waar meer in het algemeen over de taken van iRvN wordt gesproken.

[22] Omdat de colleges en gemeenteraden van de gemeenten Druten en Wijchen de aanpassing van de GR op deelname aan de ICT-module van de gemeente Wijchen niet hebben vastgesteld, kon die versie van de GR niet gepubliceerd worden en daarmee ook niet in werking treden (artikel 26 lid 4 Wet gemeenschappelijke regelingen). Pas na een volgende wijziging kon de GR gepubliceerd worden.

- GR geldig van 9 februari 2016 tot en met 31 december 2021
- GR geldig vanaf 1 januari 2022

[23] Gemeenschappelijke Regeling MGR.

geautomatiseerde systemen[24]. Het gaat hierbij om zaken zoals netwerk- en systeembeheer, softwarebeheer en technisch applicatiebeheer, ICT-inkoop en werkplekondersteuning.

Taakverdeling informatiebeveiliging: de kaders

De GR biedt de mogelijkheid kaders vast te leggen in een beleidsplan, waarin de hoofdlijnen van het beleid worden neergelegd, en een uitwerking daarvan in een jaarlijks uitvoeringsprogramma[25]. Tot nu toe is geen gebruik gemaakt van die mogelijkheid. Daar zijn dus geen kaders voor de verdeling van taken en verantwoordelijkheden te vinden.

Waar wel kaders zijn te vinden, is in de Basisafspraken ICT-diensten (verder: de Basisafspraken)[26]. Daarin is de dienstverlening van iRvN aan alle deelnemende gemeenten vastgelegd. De Basisafspraken worden een 'collectieve dienstverleningsovereenkomst' genoemd. In deze Basisafspraken ontbreekt het echter aan de meeste onderdelen die de GR voorschrijft voor een dienstverleningsovereenkomst (DVO). Zo ontbreekt het aan (SMART[27] geformuleerde) doelstellingen. Er zijn weliswaar strategische, tactische en operationele kaders opgenomen in de Basisafspraken, maar deze betreffen feitelijk niet meer dan uitgangspunten voor de uitvoering[28]. De overige in de GR voorgeschreven onderdelen voor een dienstverleningsovereenkomst komen niet terug in de Basisafspraken. Het gaat dan om Effecten, Prestaties, Kwaliteitseisen en Budgetten en risico's, zowel in financiële als in inhoudelijke zin. In de Basisafspraken wordt wel uitgebreid ingegaan op de diverse overleggen die ambtelijk op strategisch, tactisch en operationeel niveau plaatsvinden tussen de gemeenten (afzonderlijk en samen) en iRvN. Ook wordt genoemd dat de portefeuillehouders uit de deelnemende gemeenten één keer per kwartaal overleggen[29]. Het doel van de overleggen is om de kwaliteit van de gerealiseerde versus de afgesproken dienstverlening te bespreken aan de hand van kritische prestatie-indicatoren (KPI's)[30], trends en adviezen. Die KPI's zijn op dit moment nog niet geformuleerd.

Onderdeel van de Basisafspraken is een productencatalogus. Daarin is uitgewerkt welke producten en diensten iRvN levert en welke daarvan verplicht of optioneel door de gemeenten worden afgenomen. Hierbij

[24] De gemeente Nijmegen heeft ook het functioneel applicatiebeheer bij iRvN belegd. Het gaat dan om:
- het optimaal gebruik en de instandhouding van de functionaliteit van de applicatie;
- de instandhouding van de operationalisering van de applicatie, applicatieprogrammatuur en gegevensverzamelingen welke vanuit het gebruik beschikbaar moeten zijn.

[25] Het Algemeen Bestuur kan een Uitvoeringsbeleidsplan en Uitvoeringsbeleidsprogramma vaststellen (GR MGR artikel 25). Voor de module Werkbedrijf is een strategisch beleidsplan opgesteld; voor de ICT-module is dat niet gebeurd.

[26] Voor dit onderzoek hebben wij de versie van de Basisafspraken bestudeerd die gelden vanaf 1 januari 2021. In de Basisafspraken staat dat deze worden vastgesteld door het DB. Uit het versiebeheer van deze Basisafspraken en de agenda's van het DB is echter niet op te maken dat dit gebeurd is.

[27] SMART: Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden. In bijlage 7 is een uitgebreidere toelichting opgenomen.

[28] In Bijlage 5 zijn de strategische, tactische en operationele kaders uit de Basisafspraken opgenomen.

[29] In de praktijk overleggen zij twee keer per jaar. De bestuurlijke overleggen zijn toegelicht in paragraaf 3.8.

[30] In Bijlage 7 is een nadere toelichting opgenomen.

zijn ook afspraken gemaakt over aansprakelijkheid. Het ontbreekt echter aan afspraken over wie aansprakelijk is als het doen of nalaten van activiteiten door één van de deelnemers (ook) leidt tot schade bij de andere deelnemers.

Basisafspraken:

- Tactisch kader: We dragen gezamenlijk verantwoordelijkheid voor de naleving van privacy- en informatieveiligheid;
- De gemeenten zijn zelf primair verantwoordelijk voor de implementatie van de BIO. Daar waar iRvN namens hen zorgdraagt en verantwoordelijk is voor de ICT-infrastructuur, draagt zij ook verantwoordelijkheid voor de BIO-controls en maatregelen in het kader van implementatie, het beheer en het aanleveren van bewijslast voor de betreffende audits (ENSIA[31]).

Productencatalogus:

- Bij informatiebeveiliging gaat het om de beveiliging van gegevens en systemen. Dat wil zeggen, het ervoor zorgen dat de aanwezigheid en beschikbaarheid van gegevens en systemen gewaarborgd is en gegarandeerd is volgens wet- en regelgeving (zoals BIO en AVG) en dat de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau beperkt wordt. Om dit niveau te bepalen toetst iRvN nieuwe applicaties aan de BIO en AVG. De informatiebeveiliging is een verantwoordelijkheid van de gemeente zelf.

Uit de Basisafspraken en productencatalogus blijkt dat de gemeenten primair zelf verantwoordelijk zijn voor informatiebeveiliging en de implementatie van de BIO. iRvN draagt de verantwoordelijkheid voor overgedragen ICT-infrastructuur. Uit een recent advies over de ICT-samenwerking in de regio[32] en uit de gevoerde gesprekken wordt duidelijk dat deze taakverdeling een min of meer bewuste keus is geweest in de afgelopen jaren. Bij de start van iRvN in 2016 was afgesproken om te beginnen met de techniek (automatisering), en later mogelijk te verbreden met informatiseringsaspecten, zodat iRvN een informatiedienst voor de gemeenten zou gaan vormen. In de daaropvolgende jaren heeft die verbreding niet plaatsgevonden. In het adviesrapport staat het duidelijk: "Mede als gevolg van de keuze om de reikwijdte van de samenwerking te beperken tot de techniek, is er geen gemeenschappelijk I&A[33]-beleid tot stand gebracht. Daartoe zijn wel pogingen ondernomen, maar niet met het gewenste resultaat. De betrokken organisaties voeren nu ieder afzonderlijk of in een combinatie een 'eigen informatiseringsbeleid' "[34]. In het kader van dit onderzoek betekent dit dat informatiebeveiligingsbeleid grotendeels bij de individuele gemeenten is gebleven.

Is het niet-verbreden van de samenwerking en daarmee dus van het iRvN-takenpakket in het verleden een bewust bestuurlijk besluit geweest? De rekenkamers hebben niet kunnen vaststellen of en op welke manier er bestuurlijke besluitvorming in MGR-verband heeft plaatsgevonden over de verdeling van taken en verantwoordelijkheden tussen de gemeenten en iRvN. Onduidelijk is dus ook of de bestuurders van de

[31] ENSIA staat voor Eenduidige Normatiek Single Information Audit, en is een verantwoordingsstelsel voor informatieveiligheid. In paragraaf 3.6 is een toelichting opgenomen.

[32] PWC Accountants, 'Evaluatie ICT Rijk van Nijmegen en de I&A-samenwerkingspartners, met het oog op de toekomst', september 2021.

[33] I&A: Informatisering & Automatisering.

[34] Idem, p. 17.

deelnemende gemeenten dit expliciet hebben besproken en afgewogen. Feit is dat er op bestuurlijk niveau in MGR-verband weinig over de ICT-samenwerking wordt gesproken. We komen daar op terug in paragraaf 3.8 over bestuurlijke verantwoordelijkheid en commitment. We weten dus ook niet waarom er in MGR-verband geen gemeenschappelijk informatiseringsbeleid (met daarbinnen informatiebeveiligingsbeleid) is vastgesteld.

Medio 2021 heeft iRvN een document opgesteld getiteld 'IB as a service'. Doel is om te verduidelijken wat de organisatie voor de gemeenten kan en wil gaan doen op het gebied van informatiebeveiliging. Gezien de opzet en inhoud van 'IB as a service' zou het een goede basis kunnen vormen voor een door het Algemeen Bestuur (AB) vast te stellen beleidsplan voor de ICT-module. Zo ver is het echter nog niet: het document is tot op heden enkel met de hoofden bedrijfsvoering van de gemeenten besproken.

De *bewuste* besluitvorming over het verbreden van de ICT-samenwerking is er in 2022 alsnog gekomen, maar niet in MGR-verband. In 2020 en 2021 heeft PWC in opdracht van de gemeentesecretarissen van de zeven gemeenten die deelnemen in de MGR geadviseerd over de toekomstige ICT-samenwerking. In het rapport dat in september 2021 is opgeleverd, zijn twee 'sporen' voor de toekomstige ontwikkeling beschreven. Over het advies is gesproken in het portefeuillehoudersoverleg ICT van de zeven gemeenten, en begin 2022 is er over besloten door de zeven colleges. Kort samengevat is de twee sporen-benadering overgenomen. Kern daarvan is dat iRvN de technische basisvoorzieningen (het A-deel van Automatisering) blijft doen, en dat de bredere informatisering (het I-deel) georganiseerd blijft bij de gemeenten zelf. Op losse thema's kan voortaan wel worden samengewerkt, in wisselende samenstellingen. De reden om geen gemeenschappelijk informatiseringsbeleid (al dan niet binnen iRvN) te gaan ontwikkelen is, aldus het advies, dat daarvoor "de typologie en dynamiek van de deelnemers te verschillend [is] in combinatie met de wens tot de eigen autonomie". PWC spreekt daarnaast over 'nauwelijks toegevoegde waarde en eerder een afbreukrisico'[35].

Taakverdeling informatiebeveiliging: de praktijk in onze gemeenten

Het onderzoek laat zien dat er in de praktijk soms onduidelijkheid is over de afbakening van de taken en verantwoordelijkheden tussen de gemeenten en iRvN. Afgezet tegen de BIO-normen hebben de onderzoekers diverse omissies en (daardoor ook) grijze gebieden in de afspraken tussen gemeenten en iRvN geconstateerd. Heel concreet bleken ten tijde van het onderzoek geen concrete afspraken oftewel vastgesteld beleid te bestaan op de volgende gebieden:

- Organiseren van informatiebeveiliging (zoals beveiliging van mobiele apparatuur en telewerken[36]);
- Veilig Personeel (zoals screening van medewerkers van iRvN voorafgaand aan het dienstverband);
- Beheer van bedrijfsmiddelen (zoals informatieclassificatie);
- Fysieke beveiliging en beveiliging van de omgeving (zoals beveiliging computerruimten);
- Beveiliging bedrijfsvoering (zoals bescherming tegen malware, logging en audits);
- Communicatiebeveiliging (zoals het beheer van netwerkbeveiliging en informatietransport);
- Leveranciersrelaties (zoals vereisten aan het beheer van dienstverlening van leveranciers).

[35] Idem, p. 6.

[36] Inmiddels wordt gewerkt aan concrete afspraken hierover; het is de bedoeling dat die in 2022 worden geïmplementeerd.

Al in de fase van de documentenuitvraag en ook tijdens de gesprekken bleek dat er soms onduidelijkheid bestond over de vraag of de gemeente of iRvN bepaalde onder de BIO verplichte documentatie zou moeten aanleveren aan de rekenkamers. De rekenkamers hebben binnen de scope van dit onderzoek niet tot de bodem uitgezocht wie nu precies waarvoor verantwoordelijk is; dat is niet onze verantwoordelijkheid. We stellen wel vast dát er op onderdelen onduidelijkheid is. In de slotfase van het onderzoek heeft iRvN inzicht geboden in een overzicht (ISMS[37]) dat laat zien voor elk onderdeel van de BIO of er gedocumenteerd beleid bestaat, en of de gemeenten of iRvN hierover moeten beschikken. Aan dit overzicht wordt nog volop gewerkt.

Hoe komt het dat er onduidelijkheden en grijze gebieden bestaan tussen de gemeenten en iRvN? Uit de gesprekken leiden we af dat in ieder geval een deel van de onduidelijkheid wordt veroorzaakt doordat de gemeenten op allerlei deelgebieden van informatiebeveiliging geen (nader) beleid hebben vastgesteld. Voorbeelden zijn de hierboven opgesomde zaken waarover geen concrete afspraken zijn gemaakt. iRvN heeft beleid nodig om de dienstverlening aan de gemeenten goed te kunnen uitvoeren. Wat er in de praktijk gebeurt, is dat iRvN in dergelijke situaties volgens zelf vastgestelde routines en richtlijnen gaat werken, om zodoende de gemeenten te kunnen bedienen. Deze manier van werken leidt er vervolgens toe dat voor gemeentelijke medewerkers het beeld ontstaat dat deze routines door iRvN voor hen worden vastgesteld. In het adviesrapport over de ICT-samenwerking uit 2021 staat dit als volgt verwoord: "Vanuit de operationele behoefte worden technische/inhoudelijke keuzes gemaakt (bijvoorbeeld inrichting Teams, keuze en inrichting laptops, 'policies' rondom het gebruik van USB-sticks, en andere maatregelen met betrekking tot informatieveiligheid), waarbij het vooralsnog ontbreekt aan tactische beleidsafstemming. Er is geen goed vehikel beschikbaar om beleidsmatige vraagstukken met elkaar af te stemmen" [38]. Die laatste zin is zeker relevant.

De rekenkamers stellen vast dat er in het verleden al dan niet bewust is besloten om geen gezamenlijk *informatiebeveiligings*beleid in iRvN-verband te voeren. Recent (begin 2022) is daar besluitvorming door de zeven deelnemende gemeenten bijgekomen om geen gemeenschappelijk *informatiserings*beleid in bredere zin te gaan voeren, in iRvN-verband of anderszins. Hierover is niet in MGR-verband besloten, maar enkel in de colleges, op voorstel van het portefeuillehoudersoverleg. Dit rekenkameronderzoek was niet in eerste instantie gericht op de bestuurlijke besluitvorming over ICT-samenwerking in de regio, maar de rekenkamers vinden het opmerkelijk dat de discussie en de besluitvorming hierover grotendeels buiten de MGR worden gevoerd. Hoe dan ook: omdat er geen gemeenschappelijk informatiseringsbeleid (met daarbinnen informatiebeveiligingsbeleid) is, zijn de gemeenten dus grotendeels zelf verantwoordelijk voor informatiebeveiligingsbeleid. Maar in de praktijk ontbreken er bij de gemeenten op tactisch en operationeel niveau veel van de benodigde elementen van dat beleid, en krijgt iRvN op onderdelen dus onvoldoende (beleids)kaders mee. Dat leidt er (mede) toe dat er onduidelijkheid is over precieze taak- en verantwoordelijkheidsverdeling tussen gemeenten en iRvN voor informatiebeveiliging.

[37] In paragraaf 3.4 is een toelichting op het instrument ISMS opgenomen.

[38] PWC Accountants, 'Evaluatie ICT Rijk van Nijmegen en de I&A-samenwerkingspartners, met het oog op de toekomst', september 2021, p. 18.

Aanbevelingen

1. Zorg voor heldere afspraken tussen de gemeenten en iRvN over informatiebeveiliging

a. Vraag het college om zo snel mogelijk te zorgen voor een heldere taakafbakening tussen gemeenten en iRvN inzake informatiebeveiliging. Dit voorkomt risico's als gevolg van onduidelijkheid hierover, en stelt iRvN in staat de gemeenten beter en efficiënter te ondersteunen. Vraag het college over een jaar te rapporteren, liefst op basis van een extern onderzoek.
b. Vraag het college om in MGR-verband een meerjarenbeleidsplan voor de ICT-module op te stellen met daarin duidelijke doelstellingen. Vraag het college dit beleidsplan op hoofdlijnen uit te werken in een (meerjaren)uitvoeringsprogramma, waarin wordt ingegaan op de benodigde inspanningen door zowel iRvN als de gemeenten. Bijzondere aandacht verdient daarbij het opstellen van de tot nu toe ontbrekende (beleids)kaders voor informatiebeveiliging. Overweeg als raad de zienswijzen op dit meerjarenbeleidsplan gezamenlijk met de andere raden voor te bereiden.
c. Vraag het college om het DB van de MGR voortaan, op basis van het meerjarenbeleidsplan en –uitvoeringsprogramma, een jaarlijks uitvoeringsprogramma (collectieve DVO) vast te laten stellen. Vraag het college om het DB in de jaarstukken verantwoording af te laten leggen over de doelstellingen.

2. Overweeg om het pad in te slaan van gezamenlijk informatiebeveiligingsbeleid in de regio

Vraag het college om bestuurlijk de discussie aan te gaan om toch tot een gezamenlijk informatiebeveiligingsbeleid in de regio te komen. Voor de hand ligt om iRvN daarvoor te gebruiken: de organisatie staat al, en is bestuurlijk ingebed in de MGR. Een gezamenlijk beleid, waarin onder meer is vastgelegd welk gedeeld volwassenheidsniveau de gemeenten nastreven, is de beste manier om de informatiebeveiliging in onze gemeenten te vergroten en de risico's te verminderen. Laat je als raad informeren over de mogelijke keuzes en implicaties daarvan. Bij het bepalen van je standpunt hierover kun je je als gemeenteraad extern laten adviseren. Overweeg dat in regionaal verband te doen.

3.3 WETEN WAT JE PLAN IS: GEMEENTELIJK BELEID

Vereisten aan beleid en uitwerking

De landelijke kaders (te weten de BIO en de AVG) vereisen dat de gemeente (strategisch) beleid formuleert voor informatiebeveiliging en privacybescherming. Verwacht mag worden dat er op basis daarvan een uitvoeringsprogramma of meerjarenplan wordt opgesteld, en jaarplannen met concrete doelstellingen, activiteiten en benodigde middelen.

Strategisch beleid moet ook nader uitgewerkt zijn in maatregelen, richtlijnen, protocollen, procedures, standaarden etc. voor de diverse onderdelen. Voorbeelden zijn in de vorige paragraaf aan de orde gekomen. Voor een gemiddelde gemeente is dit een lange lijst met vereiste uitwerkingen, dat is kenmerkend voor dit beleidsterrein. In figuur 3 is te zien hoe het beleid uit meerdere lagen moet bestaan.

Figuur 3 De informatiepiramide toegepast op informatiebeveiliging[39]



Op dit punt past een belangrijke waarschuwing. In dit rapport wordt veel nadruk gelegd op de aanwezigheid van schriftelijke documentatie. Dat doen de rekenkamers niet omdat ze overdreven veel waarde hechten aan papieren procedures. Maar juist op de terreinen van informatiebeveiliging en privacybescherming is het van belang dat zaken schriftelijk zijn vastgelegd (gedocumenteerd), eigenaarschap is belegd en periodiek bijstelling plaatsvindt. Dat biedt houvast aan medewerkers en zorgt ervoor dat iedereen zaken op dezelfde manier interpreteert en aanpakt. Dat is ook een van de uitgangspunten van de BIO en de reden dat daarin is vastgelegd dat een groot aantal (beleids)documenten verplicht is[40]. Hetzelfde geldt voor de AVG: de hoeksteen hiervan is het accountabilityprincipe of de verantwoordingsplicht, dat inhoudt dat een organisatie moet kunnen aantonen te voldoen aan de privacybeginselen uit artikel 5 van de AVG. We voegen er nadrukkelijk aan toe dat schriftelijk vastleggen niet genoeg is. De zorg voor informatiebeveiliging en privacybescherming moet méér zijn dan een 'papieren tijger'. Maar het schriftelijk vastleggen is wel een noodzakelijke basisvoorwaarde[41].

Informatiebeveiligingsbeleid: de praktijk in onze gemeenten

De gemeenten hebben allemaal informatiebeveiligingsbeleid geformuleerd, een belangrijke vereiste die uit de BIO kan worden afgeleid. De gemeenten hebben het beleid niet of slechts beperkt uitgewerkt in jaarplannen of uitvoeringsprogramma's. De invulling van het beleid is in alle gemeenten voor verbetering vatbaar: er is sprake van onvoldoende diepgang, doelstellingen ontbreken of zijn abstract geformuleerd en lenen zich daarmee niet goed voor nadere uitwerking in processen en werkinstructies, er is onvoldoende uitgewerkt hoe risico's adequaat beheerst worden en er is niet of onvoldoende vastgelegd hoe wordt gemonitord of het beleid

[39] Uiteraard geldt deze piramide ook voor privacybescherming.

[40] In bijlage 4 is een overzicht van de verplichte BIO-documenten opgenomen.

[41] Zie ook het in de Inleiding genoemde onderscheid tussen opzet, bestaan en werking.

wordt uitgevoerd en effectief is. Zoals ook al bleek uit de vorige paragraaf is het beleid op diverse onderdelen niet nader uitgewerkt in maatregelen, richtlijnen, protocollen, procedures, standaarden etc.. We hebben het dan over de onderste laag van de informatiepiramide. Diverse aspecten van informatieveiligheid zijn niet of onvoldoende afgedekt in het beleid, ondanks het bestaan van handreikingen hiervoor bij de IBD en de AP. Een concreet voorbeeld is dat in het onderzoek in geen van de gemeenten vastgestelde kaders zijn gevonden voor logging.

Voor iRvN geldt dat de organisatie geen eigen informatiebeveiligingsbeleid heeft geformuleerd, maar als onderdeel van de Modulaire Gemeenschappelijke Regeling Rijk van Nijmegen onder het informatiebeveiligingsbeleid van de MGR valt. Dat hebben we niet in het rekenkameronderzoek betrokken. Als uitvoeringsorganisatie moet iRvN daarnaast het informatiebeveiligingsbeleid van de zeven deelnemende gemeenten uitvoeren, voor zover het de ICT-infrastructuur betreft. Als eigenaar van de MGR en iRvN moeten de gemeenten informatiebeveiligingsbeleid op de diverse aandachtsgebieden formuleren en deze kaders aan iRvN meegeven.

Als we specifiek kijken naar de gemeente Nijmegen, dan blijkt dat het Informatiebeveiligingsbeleid van de gemeente grotendeels informatief en vrij abstract van aard is. Dat geldt zowel voor de versie 2019 die gold ten tijde van de uitvoering van dit onderzoek, als voor de geactualiseerde versie die het College op 8 februari 2022 vaststelde. Ongeveer de helft van het 6 pagina's tellende Informatiebeveiligingsbeleid betreft een toelichting op wat informatiebeveiliging behelst, wat het belang en de reikwijdte ervan is en waarom er beleid voor geformuleerd wordt. In de andere helft van het plan wordt ingegaan op de visie op informatiebeveiliging en de pijlers onder het beleid. Hierbij gaat het vooral om een bevestiging van de uitgangspunten van wet- en regelgeving en algemene sturingsprincipes.

De visie in het beleid van 2019 en 2022 komt overeen, en luidt: "De komende jaren zet de gemeente Nijmegen in op het verhogen van informatieveiligheid en een verdere professionaliseren van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van de rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken".

In beide beleidsplannen zijn geen doelstellingen opgenomen. In algemene termen is als uitwerking van of toelichting op de visie aangegeven dat de gemeente "technische en organisatorische maatregelen treft om informatie te beschermen en de kwaliteit te waarborgen, wil voldoen aan wet- en regelgeving rondom informatiebeveiliging, het volwassenheidsniveau wil verhogen en er naar streeft 'in control' te zijn en blijven". Wat het volwassenheidsniveau was op het moment van vaststelling van de plannen is niet aangegeven. Ook is niet aangegeven wanneer de gemeente welk volwassenheidsniveau wil realiseren[42]. Het ontbreekt hiermee

[42] In de Rapportage Informatiebeveiliging en Privacy 2020 vonden wij de opmerking dat de gemeente streeft naar niveau 3 van het Capability Maturity Model. Dit is het niveau waarop processen zodanig goed gedefinieerd zijn dat ze ook goed

aan een belangrijk richtinggevend kader voor de uitvoering. Het streven 'in control te zijn en te blijven' is wel geconcretiseerd. In beide plannen wordt aangegeven dat de aanpak van het informatiebeveiligingsbeleid is gebaseerd op een risicoanalyse. In het beleidsplan 2022 wordt daar bij de uitwerking van 'in control zijn en blijven' ook de nadruk op gelegd[43]:

In control zijn en blijven beleidsplan 2019	**In control zijn en blijven beleidsplan 2022**
In control betekent in dit verband dat de gemeente ***weet welke maatregelen genomen zijn, dat er een controleerbare planning is van de maatregelen die nog niet genomen zijn, en die bewaakt moeten worden.*** De genomen maatregelen dragen aantoonbaar bij aan het voldoen aan de relevante wet- en regelgeving. Aantoonbaar betekent dat verantwoordelijkheden zijn vastgelegd en ***naleving zichtbaar getoetst*** wordt.	In control betekent in dit verband dat we ***weten welke risico's we lopen, we weloverwogen hier (al dan niet) maatregelen voor treffen en de voortgang daarvan bewaken.*** Een randvoorwaarde is dat de getroffen maatregelen aantoonbaar bijdragen aan het voldoen aan relevante wet- en regelgeving. Dit betekent onder andere dat verantwoordelijkheden vastgelegd zijn en de ***naleving (zichtbaar) getoetst*** wordt.
In control zijn en blijven beleidsplannen 2019 en 2022	
Vastgelegde verantwoordelijkheden gaan gepaard met bewustzijn bij de medewerkers van hun rollen en taken op het vlak van informatiebeveiliging, zodat zij deze ook waar kunnen maken. Toetsing maakt het mogelijk om lering te trekken uit resultaten en systematisch verbetering tot stand te brengen. Hiermee kunnen ook voor de langere termijn uitspraken gedaan worden over de kwaliteit en de continuïteit van de ICT omgeving van gemeente Nijmegen.	

In het informatiebeveiligingsbeleid 2022 zijn verder algemene randvoorwaarden voor het informatiebeveiligingsbeleid benoemd. Concreet gaat het om: wetgeving, de BIO en de 10 bestuurlijke principes voor informatiebeveiliging die door de VNG als aanvulling op de BIO zijn opgesteld. Vanuit deze randvoorwaarden zijn 10 uitgangspunten geformuleerd voor de gemeente Nijmegen. Ook deze zijn algemeen van aard:[44]

1. de eindverantwoordelijkheid voor informatiebeveiliging ligt bij het College van B&W, maar informatiebeveiliging is van iedereen;
2. door periodieke controle, organisatie brede planning en coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. (…);
3. informatiebeveiliging is een continu verbeterproces dat zich steeds aanpast aan veranderende omstandigheden. (…);
4. het sturen en rapporteren over de voortgang van de kwaliteit van de informatiebeveiliging gebeurt op basis van Kritieke Prestatie Indicatoren;
5. we kennen de volgende functies rondom de informatiebeveiliging: (…);
6. de gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen;

functioneren als omstandigheden veranderen, zo wordt toegelicht. Een formeel besluit hierover hebben wij niet aangetroffen.

[43] Vet / cursief door de rekenkamer om de verschillen tussen beide plannen te laten zien.

[44] In het informatiebeveiligingsbeleid 2019 waren de uitgangspunten 1 tot en met 8 opgenomen.

7. regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden getraind in het gebruik van de voor hen relevante procedures;
8. iedere medewerker (…) is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen (…) en bij vermeende inbreuken hiervan melding te maken bij de CISO[45];
9. onze informatiebeveiliging heeft invloed op en wordt ook geraakt door die van onze ketenpartners;
10. wij registreren onze incidenten en leren daarvan zodat onze ervaringen ons weerbaarder maken.

Naast het informatiebeveiligingsbeleid kent de gemeente het Manifest 'Wij zijn Open en Weerbaar Nijmegen'. Het college stelde dit in december 2018 vast als vervolg op het Programma met die naam dat in 2017 is gestart. In het Manifest zijn tien principes en acht afspraken vastgelegd over 'hoe we ons gedragen in de digitale samenleving'. Het Manifest is niet 'van de gemeente Nijmegen'. Ook diverse organisaties in de stad hebben eraan meegewerkt en het Manifest ondertekend. Het is de bedoeling dat zoveel mogelijk gegevensverwerkers in Nijmegen het Manifest ondertekenen. In het informatiebeveiligingsbeleid wordt het Manifest niet genoemd en wordt (dus) ook geen relatie met de principes en afspraken daaruit gelegd.

Het informatiebeveiligingsbeleid is zowel in 2019 als in 2022 geconcretiseerd in de 'Uitwerking informatiebeveiligingsbeleid'. Deze Uitwerking betreft een beschrijvend overzicht van de rollen, taken, bevoegdheden en verantwoordelijkheden van de verschillende betrokkenen binnen de gemeente. Daarnaast zijn de maatregelen per BIO-onderdeel beschreven. Het betreft een opsomming van (benodigde) maatregelen. Met deze uitwerking is er sprake van een belangrijke concretisering van het beleid. Het biedt een goede basis voor een (meerjaren)uitvoeringsplan voor die maatregelen die nog niet (voldoende) zijn geïmplementeerd. Een gemeente-breed (meerjaren)uitvoeringsplan ontbreekt echter. Om te kunnen (bij)sturen en om volgens het eigen beleid 'in control te zijn en te blijven' is dat wel nodig.

Sinds de zomer van 2021 wordt binnen de gemeente Nijmegen gewerkt met een actieplan gericht op het implementeren van de maatregelen naar aanleiding van het onderzoek dat de accountant sinds 2018 uitvoert naar cybersecurity en IT-beheersing[46]. In dit zogenaamde Ambitiedocument is voor de periode 2021 – 2023 per actie een planning en taakverdeling opgenomen; de rubriek 'benodigde middelen' is niet ingevuld.

Een abstract informatiebeveiligingsbeleid, een beperkt uitvoeringsplan en het grotendeels ontbreken van voortgangsrapportages maken het voor medewerkers lastig om te bepalen hoe zij (steeds beter) kunnen of moeten bijdragen aan het beschermen van de hen toevertrouwde informatie.

Privacybeleid: de praktijk in onze gemeenten

De gemeenten hebben allemaal privacybeleid vastgesteld. Voor iRvN geldt dat deze geen eigen privacybeleid heeft geformuleerd, maar als onderdeel van de Modulaire Gemeenschappelijke Regeling Rijk van Nijmegen onder het privacybeleid van de MGR valt. Dat hebben we niet in het rekenkameronderzoek betrokken. We hebben in dit deel van het onderzoek ook niet specifiek ingezoomd op iRvN als verwerker van gegevens van de gemeenten.

[45] CISO: Chief Information Officer. In paragraaf 3.5 is een toelichting opgenomen op de CISO.

[46] Een overzicht van de bevindingen die de accountant sinds 2018 rapporteerde staat in bijlage 8.

Het Privacybeleid van de gemeente Nijmegen is op 2 juni 2018 vastgesteld door het College van Burgemeester en Wethouders. Net als het Informatiebeveiligingsbeleid is het grotendeels informatief en vrij abstract van aard. Het beleidsplan start met een inleiding, waarin ook het belang van privacybeleid wordt beschreven. Toegelicht wordt dat ”op verschillende niveaus – Europees, landelijk en lokaal, behoefte bestaat aan een duidelijk kader, dat zowel voor papieren als voor digitale verwerkingen richting geeft aan de praktijk van alle dag. (…). De wet bevat normen, die samen een afwegingskader geven. Aan de hand van dat wettelijke afwegingskader moet de gemeente afwegen of een bepaalde verwerking van persoonsgegevens is toegestaan, en zo ja, onder welke voorwaarden. (…). De vraag, of een bepaalde persoonsgegevensverwerking ‘gerechtvaardigd’ is, is niet alleen een juridische (mag dit van de wet?), maar ook een ethische (willen wij dit?) afweging. (…). Bij de beantwoording van de ethische vraag geeft het college invulling en nadere richting aan deze verantwoordelijkheid.” De uitgangspunten voor het gemeentelijk handelen die in het vervolg van het beleid genoemd staan, betreffen voornamelijk een herhaling van en toelichting op begrippen en beginselen uit de AVG. Een belangrijk principe uit de wet als de omgang met datalekken ontbreekt echter. Ook wordt niet in gegaan op de samenwerking met partnerorganisaties. Dit laatste is een cruciale tekortkoming, omdat de gemeente op basis van verschillende wettelijke verplichtingen regelmatig deelneemt in het uitwisselen van (gevoelige) persoonsgegevens.
In het privacybeleid is geen visie op of strategie voor de bescherming van persoonsgegevens opgenomen. En het privacybeleid biedt geen (concrete) handvatten voor de toepassing van de normen uit de wet. Daardoor vormt het privacybeleid geen duidelijk kader; iets waar ook volgens de inleiding van het beleid nu juist behoefte aan is. Voor de uitwerking van het beleid wordt verwezen naar het Privacyreglement. De opzet en inhoud van het privacyreglement is echter vergelijkbaar met die van het privacybeleid. In 2019 is het project ‘Mijn afdeling AVG-proof’ gestart. In het kader van dit project hebben de concernmanagers de opdracht gegeven een plan op te stellen om hun afdeling AVG-proof te laten werken. Wij hebben drie van deze plannen gezien. Deze zijn vrij algemeen van aard en diverse onderdelen zijn niet ingevuld. Zo ontbreekt het onder meer aan concrete activiteiten, verantwoordelijke medewerkers en/of een planning. Toegelicht is dat de uitwerking van de plannen bij alle afdelingen is stilgevallen tijdens de coronapandemie door het verplicht thuiswerken en een herprioritering van werkzaamheden.

Naast het privacybeschermingsbeleid kent de gemeente het Manifest ‘Wij zijn Open en Weerbaar Nijmegen’. We beschreven dit al onder het informatiebeveiligingsbeleid. Net als in het Informatiebeveiligingsbeleid, ontbreekt het Manifest ook in het privacybeschermingsbeleid en wordt ook hier geen relatie gelegd tussen de uitgangspunten van het privacybeleid en de principes en afspraken uit het Manifest.

Het onderzoek naar privacybescherming heeft zich voornamelijk geconcentreerd op het sociaal domein. De kaderstelling van privacyregels en processen, en de anticipatie op de AVG binnen het sociaal domein laat een meervoudig beeld zien. Aan de ene kant ontbreekt het op veel punten aan vastgestelde documentatie die zorgt voor inrichting en sturing. Aan de andere kanten zijn er verschillende controlemaatregelen opgezet die de processen binnen afdelingen analyseren, de mate van compliance bepalen, en waar nodig corrigerende acties voorstellen. Het geheel overziend schiet de kaderstelling van privacyregels en processen, en anticipatie op de AVG binnen het sociaal domein binnen de gemeente Nijmegen echter tekort.

Voor een aantal kernprocessen zijn procesbeschrijvingen vastgesteld. Dit geldt bijvoorbeeld voor de procedures voor het verwijderen van documenten en voor inzageverzoeken. Voor het afhandelen van datalekken is er ook een procesbeschrijving, maar deze is beknopt en voldoet niet aan de eisen die de AVG daaraan stelt. Voor andere belangrijke processen ontbreken procesbeschrijvingen. Zo zijn er geen procesbeschrijvingen voor het beheer van het verwerkingsregister, voor het delen van gegevens (een verwerking die doorlopend voorkomt binnen het sociaal domein), voor het opzetten van verwerkersovereenkomsten, en voor de rechten van betrokkenen anders dan inzage. De toestemmingsformulieren die de gemeente gebruikt verschillen in opmaak en opzet. Geen van de formulieren voldoet aan de standaarden en eisen die de AVG stelt rond toestemming. Ook de convenanten en privacyprotocollen variëren in opzet en inhoud. Deze voldoen in grote lijnen aan de gangbare standaarden en wetgeving. Bij een gebrek aan handleidingen zouden de convenanten en privacyprotocollen als richtlijnen kunnen fungeren. De vraag is alleen in hoeverre medewerkers deze bestuderen. Binnen het sociaal domein zijn er veel vraagstukken, situaties, en uitzonderingen die het toepassen van privacy tot een uitdaging maken. Juist daarom is het bieden van op maat gemaakte instructies aan medewerkers een belangrijk instrument om ervoor te zorgen dat privacy maatregelen gevolgd worden.

Aanbevelingen

3. Verhelder het beleid voor informatiebeveiliging en privacybescherming

a. Vraag het college om het strategisch beleid voor informatiebeveiliging en privacybescherming te versterken door het in ieder geval aan te vullen met een visie, ambitie en speerpunten. Dit vormt ook de basis voor de bewustwording in de organisatie. Vraag het college het beleidsplan ter besluitvorming aan de raad voor te leggen.
b. Vraag het college om het strategisch beleid uit te werken in een meerjaren-uitvoeringsprogramma en in jaarplannen, waarin concrete doelstellingen en bijbehorende middelen jaarlijks worden vast- of bijgesteld.

4. Werk zo snel mogelijk de belangrijkste ontbrekende onderdelen van het beleid uit

Vraag het college om zo snel mogelijk de belangrijkste onderdelen van zowel het informatiebeveiligingsbeleid als het privacybeleid uit te werken in concrete maatregelen, richtlijnen, protocollen, procedures, standaarden etc. Belangrijk is in elk geval risicomanagement, omdat het de basis van informatiebeveiliging betreft. Hierbij hoort ook dat voor elk van die maatregelen wordt bepaald wie de verantwoordelijken zijn voor de naleving.

3.4 WETEN WELKE RISICO'S JE LOOPT: RISICOMANAGEMENT DOOR DE GEMEENTEN EN IRVN

"Informatiebeveiliging is immers risicomanagement"

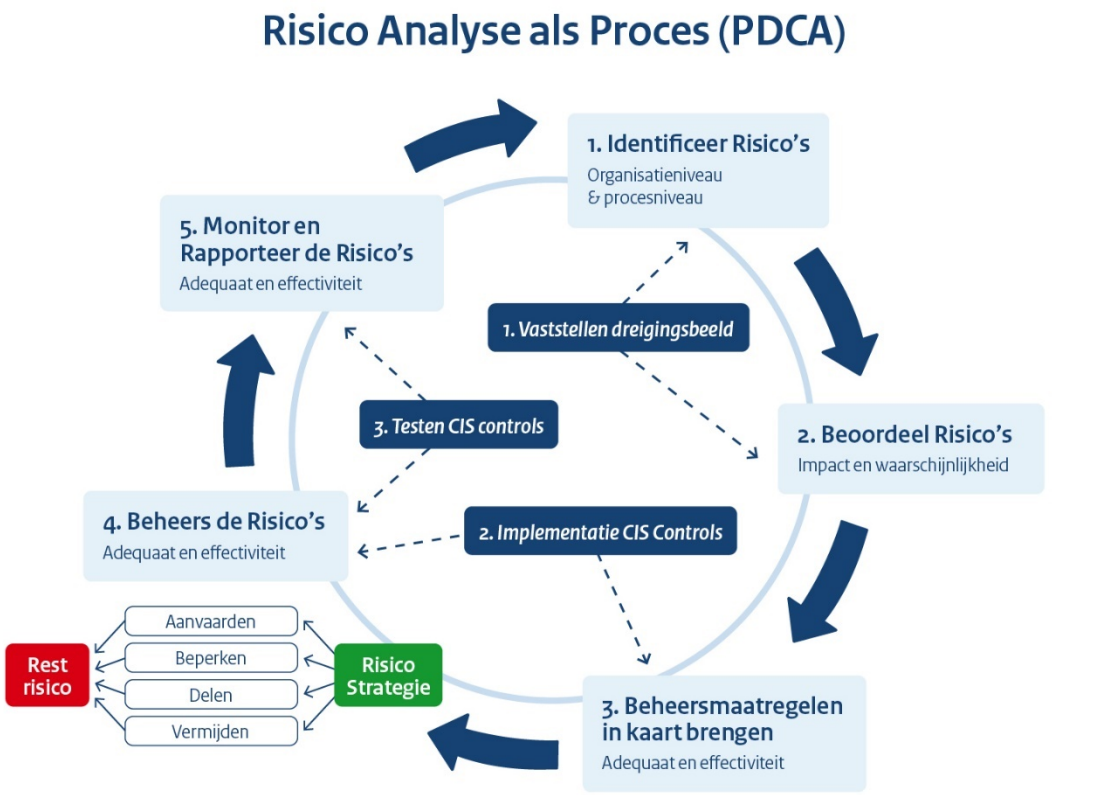
IBD - Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2021-2022, p. 3

Noodzaak van risicomanagement

"Informatiebeveiliging is immers risicomanagement" is één van de eerste zinnen in het Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2021/2022[47] van de IBD, dat is bedoeld om gemeentemanagers te helpen in hun risicomanagement. "Informatiebeveiliging is risicomanagement" is ook één van de 10 bestuurlijke principes voor informatiebeveiliging. Risicomanagement betreft een continu proces van:

- het identificeren van risico's;
- het nemen van beheersingsmaatregelen;
- het rapporteren over en monitoren van risico's;
- het treffen van maatregelen die het bereiken van doelen in de weg staan.

Figuur 4: Risicoanalyse als continu proces



CIS: Center for Internet Security. CIS is een non-profit organisatie die wereldwijd erkende "best practices" opstelt voor het beveiligen van IT-systemen en data. *Plaat: IBD*

[47] IBD Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021 / 2022.

Het is in de praktijk niet mogelijk om alle risico's uit te sluiten. "Nul risico bestaat niet" benadrukken experts op het gebied van informatiebeveiliging voortdurend[48]. Maar: het bestuur is verantwoordelijk voor het bepalen hoeveel risico en welke risico's acceptabel zijn. Dat kan alleen door goed risicomanagement. De opsomming van dreigingen en risico's in het Dreigingsbeeld 2021/2022 (zie kader) maakt duidelijk hoe belangrijk het is continu zicht te hebben op de risico's die gemeenten lopen en daar waar nodig actie op te ondernemen.

Dreigingen in volgorde van belangrijkheid:

1. Intern en onbedoeld: onbedoelde neveneffecten van logisch handelen van medewerkers, bijvoorbeeld e-mails met gevoelige informatie aan de verkeerde geadresseerde.
2. Extern, bedoeld maar ongericht: geautomatiseerde bulkaanvallen, zoals phishingmails.
3. Extern, bedoeld en gericht: gerichte aanvallen van hackers, meestal gebaseerd op onderzoek naar informatie die gebruikt kan worden bij de hack.
4. Intern en bedoeld: medewerkers die misbruik maken van hun toegangsrechten om bij gegevens of systemen te komen.

Risico's voor de ambtelijke organisatie:

- Bedrijfscontinuïteit in het geding
- Integriteit van gegevens niet gewaarborgd
- Vertrouwelijke gegevens in verkeerde handen

Risico's voor het openbaar bestuur en de politiek:

- Imagoschade
- Financiële schade
- Schade aan democratische processen

Risico's voor inwoners en ondernemers:

- Gegevens in verkeerde handen
- Dienstverlening gemeente niet beschikbaar
- Ontwrichting van alledaagse processen

Instrumenten en tools voor risicoanalyses en -management

Voor risicoanalyse en -management in gemeenten zijn diverse bekende instrumenten beschikbaar. Op het gebied van informatiebeveiliging is de GAP-analyse een standaard instrument. Het doel van een GAP-analyse is te controleren of en in welke mate de beveiligingsmaatregelen uit de BIO zijn geïmplementeerd. Als afgeleide daarvan komen ook beveiligingsrisico's in beeld. Deze vorm van analyse moet je als gemeente periodiek uitvoeren. Steeds meer gemeenten doen dit (half)jaarlijks en gebruiken de rapportages als basis voor hun jaarplannen.

Twee veelgebruikte instrumenten voor het beheren van risico's en de aanpak ervan zijn het managementinstrument ISMS, wat staat voor Information Security Management System, en de GRC-tool, wat

[48] Zie bijvoorbeeld: https://www.forumstandaardisatie.nl/nieuws/nul-risico-bestaat-niet

staat voor Governance, Risk en Compliance. Een GRC-tool is een hulpmiddel voor het beheren van de governance van een organisatie, het beheren van risico's en het naleven van regelgeving. In een ISMS wordt – volgens de principes van de PDCA-cyclus - de administratieve organisatie vastgelegd en beheerd. Beide tools ondersteunen organisaties bij de uitvoering het bijhouden en rapporteren van processen om het niveau van informatiebeveiliging te verhogen.

Een belangrijk instrument bij het beheersen van de risico's op het gebied van privacy is de zogenaamde DPIA. DPIA staat voor Data Protection Impact Assessment. De AVG eist voor bepaalde situaties, bijvoorbeeld grootschalige verwerking van persoonsgegevens, dat voorafgaand aan die verwerking wordt bepaald wat het effect van de geplande verwerkingsactiviteit is op de bescherming van de persoonsgegevens van een persoon. Als gemeente moet je dus voor allerlei processen in je organisatie zo'n DPIA uitvoeren, om inzicht te krijgen in de impact van de verwerking op de privacy. Op basis van een DPIA kunnen maatregelen worden genomen om de impact zou nodig te verminderen. Met behulp van zogenaamde pre-DPIA's kan de gemeente vaststellen welke processen als eerste aan de beurt moeten komen.

Recent heeft de IBD[49] samen met een aantal gemeenten een instrument ontwikkeld met het doel om analyses op het gebied van privacy en informatiebeveiliging eenvoudig(er) uit te kunnen voeren en overzichtelijk te kunnen presenteren en beheren: de zogenaamde Integrale Risico- en Privacy-analyse (IRPA). Binnen IRPA zijn diverse handreikingen voor analyse-instrumenten bij elkaar gebracht, zoals voor de (pre-)DPIA, de baselinetoets BIO, risicoanalyses en GAP-analyses.

De praktijk in onze gemeenten: risicomanagement informatiebeveiliging

Het risicomanagement op het gebied van informatiebeveiliging binnen de gemeenten wordt gekenmerkt door een ad-hoc karakter. Er is geen sprake van een *continu* proces van identificatie en beoordeling van risico's.

In geen van de gemeenten is een omvattend bestuurlijk besluit genomen over welke risico's wel en niet acceptabel worden gevonden, of welke prioritering nodig is bij het aanpakken van risico's.
Acceptabel zou kunnen zijn dat er voor een bepaald systeem geen aanvullende maatregelen getroffen worden, omdat de kosten daarvoor hoger zijn dan de kosten die gemaakt zouden moeten worden na een succesvolle inbreuk. Onacceptabel zou moeten zijn dat gemeentelijke IT-systemen via single-factor authenticatie benaderbaar zijn (alleen gebruikersnaam en wachtwoord).
Ook een richtinggevend ambtelijk document is in het onderzoek niet aangetroffen. In geen van de gemeenten wordt periodiek gerapporteerd over informatiebeveiligingsrisico's aan het hoogste management, het college en de gemeenteraad.

Op ad-hoc basis is er in de gemeenten aandacht voor identificatie en beoordeling van risico's. Alle gemeenten voeren in meer of mindere mate risicoanalyses uit, zoals context- en GAP-analyses. iRvN heeft in 2021 een

[49] IBD: InformatieBeveiligingsDienst.

GAP-analyse door een externe partij laten uitvoeren. Ook met de pentesten[50] en kwetsbaarheidsscans die iRvN uitvoert ontstaat inzicht in de risico's. Verder komen risico's en de mogelijke beheersing daarvan aan de orde in ambtelijke overleggen tussen de gemeente(n) en iRvN. In het geval van (dreigende) incidenten worden management, college en zo nodig ook de gemeenteraad daarover geïnformeerd. In oktober 2021 hebben de gemeenten voor het eerst een regionale crisisoefening gehouden.

Binnen de gemeente Nijmegen voert de afdeling Stadscontrol jaarlijks een gemeentebrede risicoanalyse uit. Daarin is ook aandacht voor informatiebeveiligingsrisico's. Opgemerkt moet worden dat het in deze risico-analyse gaat om het benoemen van risico's op een hoog abstractieniveau. Verder doet de accountant sinds 2018 in opdracht van de gemeenteraad onderzoek naar de cybersecurity-/ IT-beheersing. Zijn onderzoek beperkt zich tot opzet, bestaan en (waar mogelijk en relevant) de werking van de interne beheersingsmaatregelen voor zover relevant voor de controle van de jaarrekening.

Uit het onderzoek is duidelijk geworden dat tussen de gemeenten en iRvN een (althans op hoofdlijnen) duidelijke basisafspraak bestaat dat de gemeenten zelf verantwoordelijk zijn voor het risicobeleid, -beheer en -management voor wat betreft hun ICT-voorzieningen. Zij moeten zelf de GRC-tool en het ISMS vullen, maar krijgen op onderdelen gegevens aangeleverd van iRvN.

Op basis van de GAP-analyse van iRvN in 2021 wordt momenteel gewerkt aan een voorstel voor een programma waarmee de risico's op de IT-infrastructuur worden afgedekt. Hierbij worden drie scenario's onderscheiden voor het beveiligingsniveau van iRvN en de aangesloten gemeenten: een variant om op het minimaal vereiste beveiligingsniveau te komen (de basis op orde), een maximale variant en een tussenvariant. Per variant wordt beschreven welke maatregelen nodig zijn om het beveiligingsniveau in lijn te brengen met het dreigingsbeeld en wat de (jaarlijkse) kosten daarvoor zijn (materieel en personeel). Dit voorstel is in het voorjaar van 2022 besproken met de hoofden bedrijfsvoering van de gemeenten en vormt de basis voor een voorstel dat ter besluitvorming aan de colleges van de deelnemende gemeenten wordt voorgelegd.

Mogelijke verklaringen voor de ad-hoc werkwijze van de gemeenten zijn dat geen gemeenschappelijke methodiek of proces voor risicomanagement op het gebied van informatiebeveiliging is vastgesteld én dat de beschikbare instrumenten (zoals ISMS en GRC) voor het efficiënt en effectief uitvoeren van risicomanagement niet (volledig) door alle gemeenten worden gebruikt. Dit illustreert ook de inefficiënties die soms in de relatie met iRvN zitten. De gemeenten zijn in principe verantwoordelijk voor het vullen van het ISMS en de GRC-tool voor hun eigen organisatie (of het alternatief dat zij daarvoor gebruiken), maar zij hebben iRvN nodig om een deel van de benodigde gegevens aan te leveren. Omdat niet alle gemeenten hetzelfde systeem hebben aangeschaft en/of gebruiken, gaat dat minder gemakkelijk dan het zou kunnen gaan. Hierbij moet worden opgemerkt dat het (gezamenlijk) vullen nog in ontwikkeling is.

[50] Een pentest of penetratietest is een test waarbij ethische hackers proberen de systemen en netwerken van een organisatie binnen te dringen met als doel het identificeren van kwetsbaarheden en het geven van passende adviezen die kwetsbaarheden te verkleinen of op te lossen.

De praktijk in onze gemeenten: beheersen van privacyrisico's

In de gemeente Nijmegen bestaat een procedure voor de uitvoering van DPIA's en wordt geborgd dat dit gedaan wordt bij nieuwe ontwikkelingen en applicaties. In de gevoerde gesprekken is aangegeven dat er een achterstand is bij de uitvoering van DPIA's en dat deze wordt ingelopen, te beginnen met de processen met de hoogste risico-classificaties. Binnen de gemeente is er geen proces dat beschrijft hoe de monitoring van een DPIA verloopt en hoe de resultaten van de DPIA's gebruikt worden om de risicomanagementaanpak binnen de gemeente te verbeteren. In zijn verantwoording over 2021 bevestigt de FG[51] dit en noemt hij dit kwetsbaar. Verder schrijft hij dat de DPIA's nog teveel een momentopname zijn van de privacyrisico's die spelen bij een verwerking en dat de naleving van de uitgevoerde DPIA's te weinig aantoonbaar plaats vindt. Hij kondigt aan dat in 2022 de ombuiging gemaakt zal worden van implementatie naar beheer / controle. De DPIA zal dan nadrukkelijker een onderdeel gaan vormen van de (interne) verantwoordingsplicht, zo staat in de verantwoordingsrapportage over 2021.

Aanbevelingen

5. Voer zo snel mogelijk een organisatiebrede risicoanalyse uit

Vraag het college om zo snel mogelijk een organisatiebrede risicoanalyse te (laten) uitvoeren voor zowel informatiebeveiliging als privacybescherming. Kom op basis hiervan tot bestuurlijke besluitvorming over risico's die (niet) acceptabel worden gevonden en vraag het college deze te gebruiken voor het op te stellen meerjaren-uitvoeringsprogramma.

6. Maak risicomanagement tot een continu proces

Vraag het college om op korte termijn een methodiek uit te werken voor invulling van risicomanagement. Uitgangspunt voor die methodiek moet zijn dat risicomanagement als continu proces worden ingebed in de PDCA-cyclus. Blijf in het kader van risicomanagement regionale crisisoefeningen uitvoeren en gebruik de ervaringen voor de jaarplannen (regionaal én lokaal).

3.5 WETEN WAT HET KOST: INZET VAN MIDDELEN

Hoe organiseer je informatiebeveiliging en privacybescherming?

Bij het opstellen, uitvoeren en monitoren van beleid op het gebied van informatiebeveiliging en privacybescherming zijn binnen de ambtelijke organisatie medewerkers met specifieke functies nodig. Er zijn twee verplichte functies voor overheden, en dus ook voor gemeenten en gemeentelijke samenwerkingsverbanden: de CISO en de FG.

[51] FG: Functionaris Gegevensbescherming. In paragraaf 3.5 is een toelichting op de FG opgenomen.

Chief Information Security Officer (CISO)
Op grond van de BIO moet de rol van CISO belegd zijn. De CISO is verantwoordelijk voor het implementeren van het informatiebeveiligingsbeleid én het toezicht daarop. Op basis van de BIO moet de CISO zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een organisatie.
Er zitten twee kanten aan de functie van CISO: een organisatorische en een technische. De organisatorische kant heeft betrekking op het beleid, de coördinatie en de samenhang van de beveiliging. Zo helpt de CISO organisaties de kaders vast te stellen en uit te dragen, waarmee de integriteit, beschikbaarheid en vertrouwelijkheid van de informatie(voorziening) kan worden gewaarborgd. Het technische aspect van de functie betekent dat de CISO ervoor zorgt dat er maatregelen getroffen worden waardoor inbreuken op de beveiliging kunnen worden voorkomen. Of, als ze toch voorkomen, de gevolgen geminimaliseerd worden. Op basis van risicoanalyses maakt de CISO de mogelijke schade zichtbaar die een dreiging kan toebrengen aan bepaalde informatie en de kans dat het gebeurt.
De positie van de CISO dient een zekere, voor de functie noodzakelijke, onafhankelijkheid te waarborgen. Met het oog op die onafhankelijkheid adviseert de IBD[52] de CISO de beschikking te geven over een eigen budget. Korte lijnen naar het management zijn van belang om voldoende gewicht in de schaal te kunnen leggen voor het treffen en handhaven van voldoende beveiligingsmaatregelen. In tegenstelling tot de FG (zie hierna) geniet de CISO (nog) geen wettelijke ontslagbescherming.

Functionaris Gegevensbescherming (FG)
Gemeenten zijn op grond van de AVG verplicht een onafhankelijke toezichthouder aan te stellen, de FG.
De FG heeft in art. 39 AVG als taken toegewezen gekregen het informeren van de organisatie, het adviseren over verplichtingen die uit de AVG voortvloeien en toezien dat de AVG wordt nageleefd. Ook heeft de FG als taak om met de Autoriteit Persoonsgegevens (AP) samen te werken. Om deze taken goed uit te kunnen voeren moet een FG deskundig zijn op het gebied van gegevensbescherming en van de verwerkingspraktijken bij de organisatie waar hij is aangesteld. Ook moet hij verslag kunnen uitbrengen bij het hoogste leidinggevende niveau van de organisatie. De FG moet zijn taken op onafhankelijke wijze uitvoeren. Dat betekent dat de FG door de organisatie in staat moet worden gesteld met voldoende middelen zijn taak uit te voeren, dat hij geen instructies mag krijgen met betrekking tot zijn FG-taken, dat hij geen andere taken mag uitvoeren die mogelijk tot aantasting van zijn onafhankelijke positie leiden en dat hij niet mag worden ontslagen omwille van het functioneren als FG.
De FG heeft dus naast zijn rol als toezichthouder ook een rol als adviseur. Bij de invulling daarvan is van belang dat de organisatie verantwoordelijk is voor het opstellen en uitvoeren van het privacybeleid. De FG ziet toe op de naleving hiervan en brengt advies uit over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten.

De CISO en FG zijn essentiële functionarissen, maar voor goede informatiebeveiliging en privacybescherming is meer nodig in termen van organisatie en personeel. Vaak wordt daarvoor gebruik gemaakt van het zogenaamde 'Three Lines of Defense-model'[53]. Volgens dit model moeten in de organisatie drie verdedigingslijnen worden ingericht:

[52] IBD, maart 2020: Handreiking functieprofiel Chief Information Security Officer (CISO).

[53] Zie bijvoorbeeld: https://robertthart.risicomanagement.nl/2019/03/23/three-lines-of-defense-risicomanagement-model/ voor een toelichting op het model. Het model wordt ook wel kortweg Three Lines model genoemd.

1. De *eerste lijn* betreft de medewerkers in de organisatie en het management. Je kunt informatiebeveiliging en privacybescherming niet goed regelen zonder de medewerkers, die op dagelijkse basis te maken hebben met risico's en daarin keuzes maken (de proceseigenaren). Het lijnmanagement (afdelingshoofden) is in deze eerste lijn verantwoordelijk dat dit goed gebeurt.
2. De *tweede lijn* is het tactische niveau dat in de organisatie voor afstemming zorgt en de eerste lijn ondersteunt en adviseert. Op het gebied van privacybescherming betreft het de zogenaamde Privacy Officers (soms privacybeheerders of -ambassadeurs genoemd); voor informatiebeveiliging heten deze Security Officers. De tweede lijn zorgt in de diverse organisatieonderdelen voor de ontwikkeling en invoering van beleid en risicomanagement en bewaakt ook de uitvoering ervan. Daarbij hoort ook het uitvoeren van risicoanalyses
3. De *derde lijn* is die van de FG en CISO. Deze verschilt qua invulling enigszins voor de terreinen informatiebeveiliging en privacybescherming. De FG is een formele derdelijnsfunctie. Voor de CISO geldt dit (nog) niet. Bij voorkeur wordt de CISO in de organisatie ook onafhankelijk gepositioneerd en met een directe lijn (dus om de hiërarchische verhoudingen heen) naar de gemeentesecretaris en portefeuillehouder. De FG vormt het intern toezicht, vergelijkbaar met de concerncontroller in gemeenteland: hij/zij controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en moet daarover een objectief en onafhankelijk oordeel vellen, met mogelijkheden tot verbetering. De FG is ook de toezichthouder namens de AP. De CISO is wat minder een toezichthouder en vooral de strategisch adviseur van het bestuur voor informatiebeveiliging: hij/zij moet zorgen voor strategisch beleid en ook controleren of dit goed wordt geïmplementeerd. In de praktijk, dat geldt zeker in kleinere organisaties, komen de FG en de CISO niet altijd voldoende toe aan de derde lijn, omdat er in de tweede lijn nog teveel operationeel werk (voor hen) te doen is.

Wat is nodig in termen van personeel en middelen?

De rekenkamers wilden bij aanvang van het onderzoek graag duidelijkheid verschaffen aan de gemeenteraden over de inzet van de gemeenten op de terreinen van informatiebeveiliging en privacybescherming. Is er voor deze terreinen voldoende goed geschoold personeel en voldoende budget in onze gemeenten?

Die vraag kan alleen worden beantwoord met een duidelijke maatstaf.
Een eerste mogelijke maatstaf is om te onderzoeken of de informatiebeveiliging en privacybescherming helemaal op orde zijn. Als dat het geval zou zijn, kun je immers concluderen dat er voldoende mensen en middelen zijn ingezet. Maar dit is geen begaanbare weg. Los van het feit dat 100% veiligheid in feite onmogelijk is, hebben we als rekenkamers niet de onderzoekscapaciteit om een dergelijk onderzoek te (laten) verrichten. De gemeenten zouden zelf systematisch de werking c.q. effectiviteit van hun informatiebeveiligings- en privacybeschermingsbeleid moeten onderzoeken. We komen daarop terug in paragraaf 3.6.

Een tweede mogelijke maatstaf om te bepalen of de gemeenten voldoende mensen en budget inzetten, is om de input in de vorm van personeel en budget af te zetten tegen een breed gedragen norm zoals vastgesteld door experts, of tegen de inzet van andere gemeenten.

Gemeenten zijn verplicht om een FG en een CISO te hebben[54], en die op een correcte manier te positioneren in de organisatie; dat is een belangrijke wettelijke norm. Er zijn geen andere, bijvoorbeeld kwantitatieve normen voor de personele inzet beschikbaar. In 2017 stelde de Rekenkamer Rotterdam in één van de eerste lokale rekenkamerrapporten naar informatiebeveiliging dat zij geen bruikbare benchmark had weten te vinden waarmee beoordeeld kan worden een gemeente genoeg capaciteit inzet voor informatiebeveiliging[55].

Voor wat betreft het benodigde budget zijn alle deskundigen het erover eens: 'informatiebeveiliging kost geld'. Deze stelling is ook één van de 10 bestuurlijke principes die de VNG[56] voor bestuurders heeft opgesteld. De bijbehorende toelichting luidt als volgt: "Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve, repressieve en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt".

Is er iets te zeggen over de noodzakelijke omvang van het budget? De Cyber Security Raad stelde in 2017 dat overheden en andere organisaties 10% van hun IT-budget aan digitale veiligheid en privacymaatregelen zouden moeten besteden[57]. Deze zogenaamde 10 procent-maatstaf lijkt prettig concreet, maar blijkt bij nader inzien voor het onderzoek weinig bruikbaar. Onduidelijk is wat wordt bedoeld met 'bestedingen aan digitale veiligheid en privacymaatregelen'. De voor dit rekenkameronderzoek ingehuurde onderzoekers en enkele geraadpleegde deskundigen[58] geven allemaal aan dat het hier gaat om extra investeringen in maatregelen en audits, en niet om structurele uitgaven aan bijvoorbeeld personeel. Als die zouden worden meegeteld, zitten alle gemeenten sowieso al boven de 10%. Maar het is een allesbehalve helder onderscheid, vinden wij als rekenkamers. Waarom tellen de vaste personeelslasten voor de CISO en de FG niet mee, en bijvoorbeeld extra inhuur van personeel voor het treffen van bepaalde maatregelen wel? De norm lijkt al met al weinig behulpzaam.

De praktijk in onze gemeenten: personele inzet

De gemeenten hebben allemaal een CISO en een FG in dienst. De CISO's van de bij iRvN aangesloten gemeenten hebben regulier regionaal CISO-overleg, waar ook de CISO en ISO van iRvN aan deelnemen. Dit overleg kent een vaste agenda.

In de gemeente Nijmegen zijn in het document 'Uitwerking informatiebeveiligingsbeleid' de rollen en verantwoordelijkheden beschreven van de CISO en de FG, maar ook die van andere direct bij het

[54] De eerste is wettelijk verplicht op grond van de AVG; de tweede op grond van de door alle overheden onderschreven BIO-normen.

[55] Rekenkamer Rotterdam (2017). *In onveilige handen*, p.39.

[56] VNG: Vereniging Nederlandse Gemeenten.

[57] De maatstaf is gebaseerd op het adviesrapport 'De economische en maatschappelijke noodzaak van meer cyber security: Nederland digitaal droge voeten' van de commissie-Verhagen uit 2016. De commissie baseerde de norm op een internationale vergelijking.

[58] Een hoogleraar cybersecurity en een onderzoeker met ruime ervaring in onderzoek naar informatiebeveiliging bij gemeenten.

informatiebeveiligings- en privacybeschermingsbeleid betrokken functionarissen (Chief Information Officer (CIO), Security Officer (SO) en Privacy Officer (PO)). Ook de rollen en verantwoordelijkheden van het management worden beschreven. Daarbij is aangegeven door welke afdelingen het management zich voor welke onderwerpen kan laten adviseren bij het nemen van besluiten. Binnen bestaand beleid kan het management het nemen van besluiten ook aan die afdelingen mandateren. Tot slot is voor wat betreft de interne beheerorganisatie beschreven welke afdelingen primair verantwoordelijk zijn voor de uitvoering van de maatregelen. Binnen de organisatie zijn er diverse overlegstructuren tussen betrokken medewerkers. Specifiek voor privacybescherming is per afdeling een privacy-ambassadeur aangewezen. Het privacy-ambassadeurschap is een vrijwillige rol die medewerkers bekleden. Privacy-ambassadeurs dragen binnen hun afdeling het beleid uit en zijn eerste aanspreekpunt voor privacyvraagstukken.

De CISO en de FG zijn binnen de gemeente Nijmegen gepositioneerd binnen de afdeling Stadscontrol (3e lijn in termen van het Three Lines of Defence model). Zij zijn strategisch verantwoordelijk voor het houden van onafhankelijk toezicht op en adviseren van de organisatie. De SO en PO hebben een adviserende en tactisch-ondersteunende rol. De SO (aangesteld per december 2021) adviseert de concernmanagers, de CISO en CIO. De PO adviseert en ondersteunt de FG. Uit het onderzoek is naar voren gekomen dat er bij enkele medewerkers zorgen zijn of de beschikbare capaciteit voldoende is om de komende jaren alles te doen wat nodig is op het gebied van informatiebeveiliging en privacybescherming.

De praktijk in onze gemeenten: budget

De vraag of de gemeenten de 10%-norm van de Cyber Security Raad halen voor informatiebeveiliging en privacybescherming valt op basis van het onderzoek niet met hard bewijs te beantwoorden. Niet alleen is de norm onduidelijk – zoals aan het begin van deze paragraaf is toegelicht -, maar het blijkt dat de daadwerkelijke bestedingen van gemeenten aan informatiebeveiliging en privacybescherming niet goed zijn vast te stellen.

In de gemeente Nijmegen hebben we in het kader van het onderzoek met betrokken medewerkers gepoogd het totaal beschikbare IT-budget en het totale budget voor informatiebeveiliging in beeld te brengen. We hebben echter moeten vaststellen dat dit niet mogelijk bleek. Of er genoeg financiële middelen beschikbaar zijn voor informatiebeveiliging en privacybescherming, hebben we dus niet kunnen vaststellen.

Informatiebeveiliging en privacybescherming zijn geen gestandaardiseerde taakvelden in de gemeentelijke begroting, en dus valt niet of nauwelijks vast te stellen hoeveel de gemeente eraan uitgeeft. Voor zover aanwezig, zijn in de uitvoeringsprogramma's de paragrafen over de benodigde middelen niet ingevuld. Ook daar kunnen dus geen bedragen uit worden afgeleid.

Wat wel gezegd kan worden, is dat het grootste deel van de ICT-kosten de bijdrage aan iRvN betreft. In 2021 ging het in totaal om € 10.660.000: € 7.130.000 voor automatisering en € 3.530.000 voor informatie- en applicatiebeheer. Of iRvN voldoet aan de norm dat 10% van dat bedrag wordt besteed aan informatiebeveiliging, hebben we niet kunnen vaststellen.

Specifieke kosten voor informatiebeveiliging of privacybescherming (door iRvN en de gemeente) kunnen in beeld gebracht worden, maar veel kosten zitten 'verstopt' in andere posten, omdat informatiebeveiliging of privacybescherming daar een onlosmakelijk onderdeel van is. Dat geldt niet alleen voor de materiële budgetten, maar ook voor de personele lasten. Voorbeelden van dergelijke verstopte kosten zijn de aanschaf van een veiliger versie van een software-applicatie, de kosten voor de accountant voor zover die betrekking heeft op cybersecurity / IT-beheer. Verder geldt dat een deel van de inspanningen op het gebied van informatiebeveiliging en privacybescherming natuurlijk onderdeel is van de gewone werkprocessen in de organisatie, omdat de zorg hiervoor onderdeel is van het werk van alle medewerkers, en zeker ook van lijnmanagers. Die kosten zijn in feite dus elders in de begroting te vinden. De personele kosten die wel inzichtelijk te maken zijn (CISO, FG en andere direct bij informatieveiligheid en privacybescherming betrokken medewerkers), tellen juist weer niet mee in de 10% norm.

Aanbevelingen

7. Stel voldoende middelen beschikbaar

Vraag het college om de raad voor te leggen wat er nodig is qua financiële en personele middelen, op basis van het op te stellen meerjarenuitvoeringsprogramma en de jaarplannen. Die belangrijke documenten vragen om bespreking en besluitvorming in het college.

8. Geef de CISO en FG de beschikking over een eigen budget

Vraag het college om in lijn met het advies van de IBD het budget waarover de CISO kan beschikken te specificeren in het jaarplan en de begroting. Doe dat ook voor de FG. Op deze manier kunnen CISO en FG hun rol vanuit de 3e lijn beter waarmaken.

3.6 WETEN WAAR JE STAAT: TOETSING EN RAPPORTAGE

Toetsing en rapportage: hoe het moet

Voor zowel informatiebeveiliging als privacybescherming geldt dat een belangrijke vereiste voor alle (overheids)organisaties is dat opzet, bestaan en werking van de maatregelen regelmatig wordt getoetst en dat daarover wordt gerapporteerd. Het gaat hier in feite over de 'Check' in de in hoofdstuk 2 genoemde Plan-Do-Check-Act-cyclus (PDCA-cyclus), die organisaties voortdurend moeten doorlopen.

Opzet – bestaan – werking
Bij het toetsen en beoordelen van de stand van de informatiebeveiliging en privacybescherming wordt vaak naar deze driedeling gekeken:
Opzet: het ontwerp van maatregelen (in beleid, plannen en processen)
Bestaan: dat de maatregelen feitelijk zijn getroffen
Werking: de effectiviteit van de getroffen maatregelen

We kwamen ook de volgende formulering tegen:
Opzet: de aanpak klopt op papier
Bestaan: de aanpak is volgens plan in praktijk gebracht
Werking: de aanpak blijkt ook in de praktijk doelmatig en doeltreffend

In een goed georganiseerde gemeente is deze toetsing op diverse manieren georganiseerd en terug te vinden:

- In het gemeentelijk beleid moet zijn vastgelegd op welke momenten en welke manieren getoetst wordt of alle voorgenomen stappen zijn gezet en of de maatregelen effectief zijn.
- De organisatie controleert zelf (intern) of voorgenomen maatregelen zijn uitgevoerd en rapporteert daarover periodiek aan het management en de portefeuillehouder en uiteindelijk aan het college. Aan de gemeenteraad wordt verantwoording afgelegd via de gebruikelijke P&C-cyclus[59] en separaat afgesproken specifieke voortgangsrapportages.
- Ook de accountant neemt in de jaarlijkse controle informatiebeveiligingsaspecten mee. De diepgang waarmee dat gebeurt, kan sterk verschillen: per accountant, en ook per jaar, en ook afhankelijk van de vraag of en hoe de gemeenteraad deze controle toevoegt aan de opdracht.
- Minimaal verplicht moet de gemeente rapporteren over beide terreinen. Voor informatiebeveiliging is dat jaarlijks op basis van de ENSIA-systematiek (zie het volgende kader en figuur 5). Voor wat betreft de AVG moet de FG als toezichthouder rapporteren aan “het hoogste leidinggevende niveau van de verwerkingsverantwoordelijke”. In het geval van de gemeente is dit het college van B&W. Het is aan de FG zelf om te bepalen met welke frequentie hij rapporteert; gebruikelijk is minstens eenmaal per jaar.
- Op grond van de BIO[60] zouden gemeenten zelf de werking (effectiviteit) van de getroffen maatregelen regelmatig moeten onderzoeken, onder meer door middel van pentesten (penetratietesten). Die worden gedaan om op zoek te gaan naar zwakke plekken in de beveiliging van de systemen en infrastructuur. Uit de testen kunnen indien nodig verbeteracties voortkomen.
- Gemeenten doen er goed aan ook externe toetsing en controle te organiseren met een (IT-)audit door een onafhankelijke externe partij. Voor privacybescherming is dit in eerste instantie de taak van de FG, maar kan een extern uitgevoerde nulmeting of ‘privacy risk assessment’ worden uitgevoerd.

[59] Gemeenten hebben in de VNG-resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ uit november 2013 onder meer afgesproken dat in de jaarstukken een aparte passage over informatiebeveiliging wordt opgenomen.

[60] BIO 18-2-3: "Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico’s ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten."

ENSIA-rapportage
ENSIA staat voor Eenduidige Normatiek Single Information Audit, en is een verantwoordingsstelsel voor informatieveiligheid, ontstaan vanuit een gezamenlijk initiatief van de meest betrokken ministeries en de VNG. ENSIA wordt door gemeenten gebruikt om zich te verantwoorden over de staat van informatiebeveiliging op basis van de BIO en over een (groeiend) aantal landelijke voorzieningen[61].
De verantwoording over de stand van zaken van de BIO is bedoeld voor de gemeenteraad. De VNG stelt in een toelichting over ENSIA op haar website: "Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad".
De verantwoording over de landelijke voorzieningen is bedoeld voor toezichthouders binnen het Rijk. Met ENSIA wordt die verantwoording gestructureerd, zodat gemeenten maar één keer verantwoording hoeven af te leggen. Gemeenten moeten jaarlijks een zelfevaluatie invullen. Voor DigiD en Suwinet[62] moeten zij deze laten controleren door een onafhankelijke auditor. Wanneer een gemeente ook na een herstelperiode niet aan de eisen voldoet, wordt ze afgesloten van de dienstverlening. Voor de overige onderdelen geldt: het invullen van de zelfevaluatie is verplicht, het laten uitvoeren van een controle daarop (nog) niet.

Figuur 5: Schematische weergave van ENSIA-rapportage



De toetsingspraktijk in onze gemeenten
In de gemeente Nijmegen wordt een aantal zaken getoetst en gerapporteerd. In algemene zin heeft de gemeente de eerste stappen gezet om te komen tot een continue verbetercyclus (PDCA-cyclus), maar er is nog geen sprake van een volledig uitgevoerde cyclus.

Een van de uitgangspunten van het Informatiebeveiligingsbeleid is dat het sturen en rapporteren over de voortgang en de kwaliteit van de informatiebeveiliging en privacybescherming[63] gebeurt op basis van

[61] De Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).
[62] Suwinet is een digitale infrastructuur waarmee de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.
[63] In het Privacybeleid wordt niet specifiek ingegaan op het (bij)sturen en rapporteren over de uitvoering. In zijn algemeenheid is aangegeven dat het Privacybeleid onder meer in lijn is met het Informatiebeveiligingsbeleid.

Kritische Prestatie Indicatoren (KPI's). Daar wordt geen invulling aan gegeven. Er zijn geen KPI's geformuleerd en er worden gedurende het jaar geen voortgangsrapportages opgesteld.

Tijdens de uitvoering van dit rekenkameronderzoek voerde de FG met behulp van checklists van de AP een toets uit op getroffen maatregelen en op de kwaliteit en naleving van die maatregelen. Aangegeven is dat hij het resultaat begin 2022 gedeeld met het GMT[64] en verwoord heeft in de Rapportage informatiebeveiliging en Privacy 2021. Die Rapportage is door het college gedeeld met de gemeenteraad. In paragraaf 3.9 gaan we daar inhoudelijk op in.

Of en in hoeverre maatregelen worden uitgevoerd, wordt vastgelegd in een geautomatiseerd programma (ISMS, zie voor een toelichting paragraaf 3.4). Een ISMS is een belangrijk hulpmiddel bij de toetsing van de praktijk. Tijdens de uitvoering van ons onderzoek werd dit programma nog ingericht. In de verantwoordingsrapportage 2021 is aangegeven dat de inrichting is afgerond en de afdelingen het programma nu kunnen gaan vullen en beheren.

Aangegeven is dat het GMT informatieveiligheid en privacybescherming regelmatig op de agenda heeft staan; en dat het ook onderwerp van gesprek is in de prestatiedialoog[65]. Via de jaarstukken, de ENSIA-rapportage en een jaarlijkse 'rapportage informatiebeveiliging en privacybescherming' wordt de raad geïnformeerd over de voortgang. Voor de inhoud en informatiewaarde van deze stukken verwijzen we naar paragraaf 3.9 over de rol van de raad.

Informatiebeveiligingsincidenten worden geregistreerd. Er vindt echter geen (gedocumenteerde) trendanalyse van informatiebeveiligingsincidenten plaats en er is geen overzicht van (mogelijke) verbeteracties die voortvloeien uit informatiebeveiligings-incidenten. Logbestanden worden niet (geautomatiseerd) gecontroleerd op afwijkingen. In opdracht van de gemeente worden geen penetratietesten uitgevoerd om technische kwetsbaarheden te identificeren op eigen applicaties of bij iRvN[66]. Wel voert iRvN structureel kwetsbaarhedenscans uit op de technische infrastructuur waarvoor zij verantwoordelijk is. Er wordt niet gerapporteerd aan het GMT, het college of de raad over technische kwetsbaarheden.

De gemeente voert geen interne audits uit voor de BIO. Op onderdelen worden externe audits uitgevoerd. Het gaat hierbij onder meer om het onderzoek van de accountant in het kader van zijn controle van de jaarrekening en bepaalde (niet alleen de verplichte) processen die vallen onder ENSIA.

[64] GMT: Gemeentelijk Management Team.

[65] Prestatie-dialoog: periodiek gesprek tussen directeur en concernmanager.

[66] Voor DigiD is het verplicht dit te doen en gebeurt het wel.

Aanbevelingen

9. Leg vast hoe je gaat toetsen en rapporteren

Vraag het college om in het beleid op te nemen hoe je als gemeente wilt gaan toetsen en rapporteren. Neem de PDCA-cyclus als uitgangspunt en expliciteer de momenten waarop getoetst en gerapporteerd wordt. Belangrijk bij het toetsen is dat periodiek pentesten worden uitgevoerd en periodiek extern getoetst wordt. Belangrijk bij het rapporteren is dat – na overleg met de raad (zie aanbeveling 16) - ook wordt aangegeven hoe en wanneer aan de raad gerapporteerd wordt. Maak in het college (en ook in de raad, zie paragraaf 3.9) in elk geval meer werk van de jaarlijkse verantwoordingsrapportage over informatieveiligheid en privacybescherming; leg daarbij ook een relatie met de bevindingen van de accountant. Nodig de CISO en FG uit voor een toelichting en bespreking.

10. Ga KPI's gebruiken

Vraag aan het college om in het beleid KPI's op te nemen, zowel voor informatiebeveiliging als privacybescherming. Dit moet ook in de Basisafspraken met iRvN worden gedaan. Gebruik bijvoorbeeld de aandachtsvelden uit het NOREA-volwassenheidsmodel en de thema's uit de privacy-baseline om KPI's uit af te leiden.

3.7 WETEN HOE BELANGRIJK HET IS: BEWUSTWORDING

Bewustwording: essentieel onderdeel personeelsbeheer

Voor zowel informatiebeveiliging als privacybescherming is het essentieel dat medewerkers zich bewust zijn van de risico's en hun verantwoordelijkheid. Medewerkers zijn belangrijke, zo niet de belangrijkste schakels: een organisatie kan het technisch en organisatorisch nog zo goed op orde hebben, als medewerkers niet alert zijn en de richtlijnen en tips niet begrijpen of volgen, kan het alsnog mislopen. In de BIO en in de AVG zijn hier expliciete bepalingen over opgenomen.

BIO Norm 7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

AVG artikel 39 taken van de FG
1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
b) toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, ***bewustmaking en opleiding van het bij de verwerking betrokken personeel*** en de betreffende audits.

De praktijk in onze gemeenten

Uit de gesprekken blijkt dat informatiebeveiliging en privacybescherming in toenemende mate onderwerp van aandacht zijn in de gemeentelijke organisatie. Veiligheid en alertheid komen op diverse plekken en momenten ter sprake en er is sprake van een toenemend bewustzijn bij medewerkers.

Alle gemeenten ondernemen, soms ook in regionaal verband, diverse activiteiten om de bewustwording van medewerkers rond informatiebeveiliging en privacybescherming naar een hoger plan te tillen. Voorbeelden hiervan zijn: het delen van informatie, tips en waarschuwingen via intraweb, het geven van presentaties (door externen), het organiseren van quizen en het uitvoeren van phishingsimulaties. In alle gemeenten bestaan ook e-learning modules. In de gemeente Nijmegen zijn medewerkers sinds de zomer van 2021 verplicht deze te volgen. In diverse gevoerde gesprekken is aangegeven dat het aantal meldingen van (mogelijke) informatiebeveiligingsincidenten en datalekken door de bewustwordingsactiviteiten is toegenomen.

Wat ontbreekt is een systematische, gerichte aanpak, inclusief evaluatie en consolidatie. De activiteiten die de gemeenten ondernemen zijn vrijwel altijd gericht op alle medewerkers; er is weinig sprake van maatwerk voor specifieke groepen medewerkers. De meeste activiteiten betreffen eenmalige acties of korte impulsen. Of de uitgevoerde activiteiten het gewenste resultaat hebben opgeleverd, is niet bekend. Dat komt doordat het gewenste resultaat vooraf niet is vastgelegd, en achteraf wordt dit niet gemeten.

Aanbevelingen

11. Zet volop en systematisch in op bewustwording

Vraag het college om door te gaan op de weg van het vergroten van de bewustwording van medewerkers en dit meer systematisch aan te pakken, door ook hierbij te werken op basis van een risicoanalyse en volgens de PDCA-cyclus. Vraag het college bewustwording vanaf 2023 op te nemen als onderdeel van de jaarplannen voor informatiebeveiliging en privacybescherming, en daarbij ook aandacht te hebben voor bewustwordingsmaatregelen voor specifieke groepen medewerkers.

3.8 WETEN DAT JE VERANTWOORDELIJK BENT: BESTUURLIJKE VERANTWOORDELIJKHEID EN COMMITMENT

Bestuurlijke verantwoordelijkheid vereist

Omdat informatiebeveiliging en privacybescherming vaak als bedrijfsvoering worden beschouwd, en omdat het om ingewikkelde en technische materie gaat, is de kans groot dat veel bestuurders net als gemeenteraden (zie volgende paragraaf) weinig affiniteit en betrokkenheid voelen bij deze onderwerpen. Dat is misschien begrijpelijk, maar onwenselijk: bestuurders hebben een belangrijke verantwoordelijkheid als het gaat om het bevorderen van informatiebeveiliging en privacybescherming in hun gemeente. De experts waar de rekenkamers mee hebben gesproken wijzen erop dat het een zwaar portefeuilleonderdeel is voor bestuurders, en dat zij er vaak mee worstelen.

In de 10 bestuurlijke principes voor informatiebeveiliging die de VNG in 2019 aan haar leden heeft meegegeven, zie je dan ook dat het eerste principe direct aan hen is gericht: 'Bestuurders bevorderen een veilige cultuur'. Benadrukt wordt dat de bestuurder een voorbeeldfunctie heeft, dat hij/zij het beleid actief moet uitdragen en ervoor moet zorgen dat medewerkers zich vrij voelen om risico's te melden en maatregelen voor te stellen. Zoals de IBD het formuleert: "Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel" [67].

De bestuurlijke praktijk in onze gemeenten

In het onderzoek is in beperkte mate aandacht besteed aan de invulling van de bestuurlijke verantwoordelijkheid voor informatiebeveiliging en privacybescherming. In welke mate en op welke wijze de portefeuillehouders en de colleges tijd en aandacht besteden aan de sturing op deze terreinen, is niet systematisch onderzocht. Er is wel met de portefeuillehouders gesproken, en in de documenten en de andere interviews is op diverse manieren materiaal verzameld over de manier waarop de colleges van onze gemeenten invulling geven aan hun bestuurlijke verantwoordelijkheid.

Het onderzoek laat zien dat de besturen van alle vier gemeenten zich bewust zijn van het belang van de thema's informatiebeveiliging en privacybescherming. Maar de meesten van hen kennen niet de eerdergenoemde 10 bestuurlijke principes voor informatiebeveiliging van de VNG, en laten zich daar niet door leiden in hun werk. De portefeuillehouders geven aan de wettelijke vereisten, dat wil zeggen de BIO en de AVG, als leidend te beschouwen, maar zij geven daarbij aan zelf geen scherp beeld te hebben in hoeverre de gemeente daar inmiddels aan voldoet.

In de gemeente Nijmegen spreken de portefeuillehouders regelmatig met de verantwoordelijke ambtenaren op strategisch niveau (FG en CISO). Zij gaan er van uit dat de verantwoordelijke beleidsmedewerkers proactief 'aan de bel trekken' als zaken aandacht of nadere besluitvorming behoeven en zij vertrouwen in belangrijke mate op hun inzichten en prioritering van wat er moet gebeuren. In het onderzoek is onvoldoende systematisch materiaal verzameld over de vraag of van ambtelijke zijde dat vertrouwen ook zo wordt beleefd. De portefeuillehouders voelen zich verantwoordelijk voor de informatievoorziening aan hun gemeenteraad, en hebben goed zicht op de mate waarin en de manier waarop de raad betrokken is bij de beide onderwerpen.

De bestuurlijke praktijk op regionaal niveau

De gemeenten in het Rijk van Nijmegen hebben zoals gezegd hun ICT-taken belegd bij iRvN, één van de modules van de Modulaire Gemeenschappelijke Regeling (MGR) Rijk van Nijmegen. Er is bewust gekozen voor gemeenschappelijkheid op dit gebied, omdat "de structuur van een Gemeenschappelijke Regeling waarborgen geeft voor de gemeenschappelijke belangenafweging ten behoeve van alle deelnemers. In de samenstelling van Algemeen Bestuur (AB) en het Dagelijks Bestuur (DB), alsook in de verantwoordelijkheid van deze twee

[67] Uit het voorbeeld Strategisch Gemeentelijk Informatiebeveiligingsbeleid BIO van de IBD (pagina 4).

bestuursorganen zit de waarborg dat iRvN daadwerkelijk blijft functioneren binnen de opdracht om het beheer van de regionale ICT-infrastructuur op basis van gemeenschappelijkheid (harmonisatie en standaardisatie) te optimaliseren" [68]. Aangetekend moet worden dat de gemeenten slechts in beperkte mate hun beleid op dit gebied hebben geharmoniseerd. In paragraaf 3.2 over afspraken tussen de gemeenten en iRvN is dit al toegelicht.

De besluitvorming binnen de MGR vindt plaats in het AB. Op dit moment bestaat het AB uit burgemeesters en wethouders uit de deelnemende gemeenten met in hun portefeuille Werk, ICT of iets anders. In de praktijk vergadert het AB zo'n vier tot vijf keer per jaar. De vergaderingen van het AB zijn openbaar. De ICT-module (iRvN) stond in 2020 en 2021 slechts twee keer als specifiek punt op de agenda[69]. Naast het AB kent de MGR ook een DB. Het DB heeft een portefeuillehouder voor ICT. In de vorige raadsperiode was dat een wethouder van de gemeente Wijchen. Deze overlegt in principe eenmaal per zes weken met de directeur van iRvN. Omdat de DB-vergaderingen niet openbaar zijn, weten we niet of en hoe ICT en iRvN daar vaak aan de orde komen. De DB-besluiten uit 2020 en 2021 die openbaar gemaakt zijn, gingen niet over ICT of iRvN.

De MGR kent verder één adviescommissie, de Agendacommissie, bestaande uit raadsleden uit de deelnemende gemeenten. De Agendacommissie heeft tot taak de politieke besluitvorming door de raden te faciliteren. De agendacommissie vergaderde in 2020 en 2021 zeven, respectievelijk zes keer. Informatiebeveiliging en privacybescherming stonden nooit als specifiek punt op de agenda. Wel is de commissie eind 2021 mondeling geïnformeerd over het proces van de evaluatie van en advisering over de ICT-samenwerking in de regio.

De portefeuillehouders ICT uit de deelnemende gemeenten kwamen tot voor kort gemiddeld twee keer per jaar bij elkaar voor overleg. Recentelijk is de frequentie van overleg toegenomen, mogelijk naar aanleiding van het in 2021 verschenen adviesrapport over de ICT-samenwerking in de regio. In het portefeuillehoudersoverleg ICT worden formeel geen besluiten genomen.

Dat ICT of iRvN zelden op de AB-agenda staat, komt overeen met het beeld dat uit de interviews met de portefeuillehouders oprijst. Die geven aan dat ICT en iRvN niet als een politiek belangrijk onderwerp worden beschouwd. De bestuurlijke aandacht binnen de MGR gaat vooral uit naar het Werkbedrijf, de andere module van de MGR. Dit beeld wordt ook bevestigd door de afspraken die er tussen de gemeenten en iRvN zijn gemaakt. Daaruit blijkt dat er voor iRvN geen aparte bestuurscommissie is ingesteld omdat, zo staat in de Basisafspraken, iRvN "actief is op een aspect van de (ondersteuning) van de bedrijfsvoering van de deelnemende partijen en niet op een beleidsveld". Om deze reden is er voor gekozen het opdrachtgeverschap voor iRvN bij de gemeentesecretarissen neer te leggen. Maar uit het adviesrapport over de ICT-samenwerking in de regio blijkt dat "in de praktijk geen invulling wordt gegeven aan de opdrachtgevende functie van de gemeentesecretarissen. Besluiten worden meestal door de hoofden bedrijfsvoering genomen (…). Het hoofden

[68] Bron: Basisafspraken ICT-diensten Deelnemers MGR – iRvN (versie 2021).

[69] Het ging om: Voortgang evaluatie en toekomst iRvN / ICT-dienstverlening (8 juli 2021) en Voortgang onderzoek iRvN en taakstelling iRvN (1 oktober 2020).

bedrijfsvoerings-overleg blijkt daarmee een cruciale schakel in het doorzetten van adviezen en besluiten, terwijl er geen duidelijke link met het AB en DB is"[70]. De governance op regionaal niveau is dus niet goed geregeld.

Het gebrek aan bestuurlijke aandacht heeft gevolgen voor de dagelijkse praktijk van de samenwerking en afstemming tussen de gemeenten en iRvN. Het zorgen voor duidelijkheid en heldere kaders is een verantwoordelijkheid van de gemeentebestuurders. In het eerdergenoemde adviesrapport staat de in dit verband relevante passage: "Bestuurlijke borging van gemaakte keuzes m.b.t. inhoudelijke vraagstukken ontbreekt vaak. De vraagstukken worden relatief technisch aangevlogen (soms moet dit ook) terwijl soms bestuurlijke keuzes (nog) gemaakt moeten worden, maar natuurlijk ook omdat (zoals hiervoor beschreven) de tactische en strategische kaders eenvoudigweg ontbreken. Daarnaast worden bestuurders beperkt meegenomen in de I&A-ontwikkelingen en geven geïnterviewden aan dat het kennisniveau van bestuurders op het gebied van ICT en digitalisering niet toereikend is om de consequenties te bepalen van beleidskeuzes."

Deze tekst sluit naadloos aan bij de constateringen eerder in dit rapport, in paragraaf 3.2 over de afspraken en taakverdeling tussen de gemeenten en iRvN. Daaruit bleek al dat er onduidelijkheden ('grijze gebieden') zijn in de onderlinge taakverdeling, en dat de ontbrekende gemeentelijke (beleids)kaders het werk er voor iRvN niet gemakkelijker op maken.

Aanbevelingen

12. Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming *in de gemeente*

Vraag het college – in lijn met VNG-resolutie 2021 en de 10 bestuurlijke principes voor informatiebeveiliging - om de portefeuilles informatiebeveiliging en privacybescherming voldoende gewicht te geven en systematisch aandacht te besteden in de collegevergaderingen aan zaken zoals risico's, beleid, prioritering, benodigde middelen, jaarplannen, monitoring, voortgangs- en verantwoordingsrapportages en de eigen bewustwording. Het is verstandig regelmatig de CISO en FG uit te nodigen voor een toelichting.

13. Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming *in de regio*

Versterk en verduidelijk de governance op regionaal niveau. Vraag het college om in MGR-verband voldoende gewicht te geven aan de rol van IRvN bij de informatiebeveiliging in de gemeenten (en bij iRvN zelf). Dat betekent periodieke aandacht in het AB en in de Agendacommissie van de MGR voor informatiebeveiliging, zowel als het gaat om beleidsplan en jaarplannen (Plan) en rapportages (Check). Ook (of: juist) als de aansturing van iRvN bij de gemeentesecretarissen en/of hoofden bedrijfsvoering ligt, zorg dan voor noodzakelijke bestuurlijke besluitvorming in het AB. Vraag aan het college om de instelling van een aparte bestuurscommissie voor iRvN in het AB van de MGR te overwegen. Het voordeel van een bestuurscommissie

[70] PWC Accountants, 'Evaluatie ICT Rijk van Nijmegen en de I&A-samenwerkingspartners, met het oog op de toekomst', september 2021, p. 18.

ten opzichte van het werken in het portefeuillehoudersoverleg ICT is immers dat op deze manier de besluitvorming bestuurlijk is ingebed in de MGR, transparanter is en meer garanties geeft voor betrokkenheid van de gemeenteraden. Vraag het college de raad te informeren over de gehanteerde afwegingen en besluitvorming.

3.9 WETEN HOE JE STUURT EN CONTROLEERT: DE ROL VAN DE GEMEENTERAAD

Behalve op de vraag wat de colleges doen, heeft dit rekenkameronderzoek zich ook welbewust gericht op de gemeenteraden. De doelstelling van het onderzoek was tweeledig:

- Voor de gemeenteraden inzichtelijk maken hoe de informatiebeveiliging en privacybescherming door hun eigen gemeente ervoor staat, en hoe daaraan wordt gewerkt in hun gemeente[71];
- De gemeenteraden ondersteunen bij de kaderstelling en controle op dit vlak. Een belangrijke voorwaarde voor een goede rolvervulling is de informatievoorziening door het college.

In dit hoofdstuk gaan wij nader in op deze tweede doelstelling. We beantwoorden drie vragen:

1. Wat is in het algemeen de rol van een gemeenteraad op de terreinen informatiebeveiliging en privacybescherming?
2. Op welke wijze verloopt in de praktijk het proces van kaderstelling en controle door de gemeenteraad t.a.v. informatiebeveiliging en privacybescherming? Op welke wijze faciliteert het college de kaderstelling en controle door de gemeenteraad, met name qua informatievoorziening aan de raad?
3. Zijn er elders in het land relevante best practices ten aanzien van een goed verlopend proces van kaderstelling en controle door de gemeenteraad op dit gebied, en wat zijn de belangrijkste lessen die daaruit kunnen worden geleerd?

Wat is de rol van een gemeenteraad?

Voordat we toekomen aan de bevindingen van het onderzoek, moet de vraag worden beantwoord welke rol een gemeenteraad eigenlijk heeft op de terreinen informatiebeveiliging en privacybescherming. Deze vraag wordt door betrokkenen in en om het lokaal bestuur verschillend beantwoord, zo hebben de rekenkamers gemerkt. Desalniettemin zijn er enkele duidelijke uitgangspunten.

Rollenscheiding college-raad

De rollenscheiding tussen raad en college betekent dat het college (samen met de ambtelijke organisatie) belast is met het dagelijks bestuur in de gemeente. De gemeenteraad is het hoogste orgaan van de gemeente, en stelt de kaders waarmee het college van B&W moet werken (kaderstellende rol). Met 'de kaders' bedoelen we de lokale regelgeving, de hoofdlijnen van beleid en de financiële kaders. De tweede hoofdtaak van de gemeenteraad is het controleren van het bestuur (controlerende rol). De vastgestelde kaders zijn daarbij een uitgangspunt, maar de raad controleert het college in brede zin, dus op alle onderdelen van het gevoerde bestuur inclusief de uitvoering.

[71] Zie hiervoor de paragrafen 3.2 tot en met 3.8.

Raad ook verantwoordelijk voor informatiebeveiliging en privacybescherming
Informatiebeveiliging en privacybescherming worden in de gemeentelijke praktijk vaak onder bedrijfsvoering geschaard. Dat betekent **niet** dat de gemeenteraad zich er niet mee bezig mag of moet houden. Dat is een vaak gehoord misverstand. Het tegendeel is waar: samen met het college is de raad verantwoordelijk voor een goede en stabiele dienstverlening aan burgers en bedrijven, voor goed en stabiel bestuur door de gemeente en voor bescherming van de gegevens van burgers. De rollenscheiding tussen college en raad betekent wel dat de gemeenteraad niet beslist over de uitvoering van beleid en de bedrijfsvoering. Maar in zijn controlerende rol kan de raad daar altijd naar vragen en een oordeel over vellen. En de raad moet ook goed worden geïnformeerd over de uitvoering van beleid en de bedrijfsvoering, om te kunnen controleren of het goed gaat. Dat geldt bij uitstek voor de belangrijke onderwerpen informatiebeveiliging en privacybescherming, omdat die rechtstreeks van belang zijn voor de inwoners.

Geen gemakkelijke taak voor de raad
Omdat de gemeenteraad uiteindelijk verantwoording verschuldigd is aan de inwoners over het gevoerde bestuur, moet hij serieus invulling geven aan zijn kaderstellende en controlerende rol. Dat is geen gemakkelijke opgave op de terreinen informatiebeveiliging en privacybescherming: het betreft ingewikkelde, deels specialistische en technische materie, waarvan de meeste raadsleden geen verstand hebben. Net als de meeste bestuurders overigens, maar dat terzijde. Toch moet de raad het bestuur namens de inwoners hierop controleren.

Dat betekent dat de gemeenteraad zich moet (laten) informeren over de ‘basics’ op het terrein van informatiebeveiliging en privacybescherming, om te kunnen begrijpen wat er nodig is. En vervolgens is goede informatievoorziening nodig over de wijze waarop de gemeente hiermee in de praktijk omgaat. Die informatie moet worden geleverd door het college. Het college is verplicht om dat te doen in het kader van de P&C-cyclus en de ENSIA-rapportage (zie voor een uitgebreidere toelichting paragraaf 3.6). Het verplichte deel daarvan is echter beperkt, en biedt in kale vorm onvoldoende informatie voor gemeenteraden. De gemeenteraad doet er goed aan om in overleg te gaan met het college hoe hij (nader) wil worden geïnformeerd.

De praktijk: de rol van de raad en de informatievoorziening
In de gemeente Nijmegen vult de gemeenteraad zijn kaderstellende rol vrij passief in. Het beleid op het gebied van informatiebeveiliging en privacybescherming is tot nu toe vastgesteld door het college en niet door de gemeenteraad. De gemeenteraad is door het college ook niet geïnformeerd over de vaststelling van dit beleid. Recent (1 februari 2022) heeft het college een Startnotitie aan de raad gestuurd om – in samenspraak met de raad - te komen tot nieuw beleid voor informatiebeveiliging en privacybescherming. Toegelicht is dat het daarbij vooral zal gaan om de politieke vraagstukken rond digitalisering en niet of nauwelijks om bedrijfsvoeringsvraagstukken.

De kaderstelling door de gemeenteraad verloopt vooral via de gemeentelijke begroting. In de begroting 2022 is op een aantal plaatsen ingegaan op informatiebeveiliging en privacybescherming: het programma Bestuur en Organisatie, en de paragrafen Bedrijfsvoering, Verbonden partijen en Weerstandsvermogen en

risicobeheersing. De teksten zijn algemeen[72]; er zijn geen doelstellingen geformuleerd waarmee de raad het college bij de jaarstukken kan controleren. Er wordt ook niet teruggekomen op de uitgangspunten uit het informatiebeveiligings- en privacybeschermingsbeleid. In het overzicht met links naar relevante stukken, ontbreken de links naar het informatiebeveiligings- en privacybeschermingsbeleid. Meer in zijn algemeenheid vraagt de auditcommissie in haar jaarlijkse adviesbrieven bij de begroting aandacht voor dergelijke punten.

Specifiek hebben vragen van de raad in 2021 over het gebruik van 'anonieme accounts' door de gemeente geleid tot het vaststellen van richtlijnen hiervoor door het college. Meer in het algemeen vraagt de raad in debatten over zaken die raakvlakken hebben met informatieveiligheid en privacybescherming regelmatig aandacht voor privacy. Dat doet hij ook naar aanleiding van veiligheidsincidenten elders.

De controle door de gemeenteraad verloopt vooral via de jaarstukken en de ENSIA-rapportage. In de raadsperiode 2018-2022 vormden informatiebeveiliging en privacybescherming een belangrijk thema voor de auditcommissie. Vooral rond de jaarstukken heeft de auditcommissie een actieve rol gepakt om de informatievoorziening aan de raad te verbeteren. Het thema is daarmee bij de raad steviger op de kaart gezet en heeft ook geleid tot specifieke opdrachten van de raad aan het college.

De informatievoorziening in de jaarstukken is beperkt. Het ontbreekt grotendeels aan *verantwoordings*informatie. Het gaat vooral om beschrijvingen van uitgevoerde activiteiten, meer algemene toelichtingen en op onderdelen gaat het letterlijk om dezelfde teksten als in de begroting. Dit maakt een goede controle door de gemeenteraad niet echt mogelijk. Met het geven van de opdracht aan de accountant om in zijn controle ook specifiek te kijken naar de cybersecurity/IT-beheersing, heeft de raad georganiseerd dat hij toch een beeld krijgt van de stand van de informatiebeveiliging en privacybescherming[73]. De accountant doet verslag van zijn bevindingen in de boardletter en bespreekt deze met de auditcommissie. In de loop der jaren heeft de accountant, behalve voor specifieke tekortkomingen, ook meermaals aandacht gevraagd voor het opstellen van een uitvoerings- of actieplan voor de implementatie van noodzakelijke verbeteringen naar aanleiding van zijn bevindingen. Op aandringen van de auditcommissie is in de zomer van 2021 zo'n plan opgesteld (Ambitiedocument 2021 – 2023). Dit plan is door de auditcommissie besproken met betrokkenen uit de ambtelijke organisatie. Het is de bedoeling zo ook in gesprek te gaan over de voortgang van de uitvoering van het plan. Op 19 april 2022 heeft het college een brief aan de raad gestuurd, waarin – in beschrijvende en algemene zin - wordt ingegaan op de uitvoering van het plan (en enkele andere uitgevoerde activiteiten).

In het kader van ENSIA informeert het college de raad door toezending van de Collegeverklaring ENSIA en een Rapportage Informatiebeveiliging en Privacy. In de Collegeverklaringen wordt ingegaan op de mate waarin de gemeente voldoet aan de normen voor Suwinet en DigiD. Met de 'Rapportages Informatiebeveiliging en Privacy' wordt de raad 'bijgepraat' over uitgevoerde activiteiten. Ook is een

[72] Voor details uit de stukken waar in deze paragraaf naar verwezen wordt, verwijzen wij naar bijlage 8.

[73] De accountant kijkt in het kader van deze opdracht van de gemeenteraad niet gemeente-breed naar cybersecurity / IT beheersing. Hij kijkt naar die zaken die relevant zijn voor zijn controle van de jaarrekening.

vooruitblik op de komende jaren opgenomen. Er wordt in die rapportages geen directe relatie gelegd met de BIO - wat juist de bedoeling is van ENSIA - en ook niet met de uitgangspunten van het gemeentelijke informatiebeveiligings- en privacybeschermingsbeleid. Er wordt ook niet gerapporteerd aan de hand van KPI's. Dat is opvallend, omdat één van de uitgangspunten van het informatiebeveiligingsbeleid (2019 én 2022) is dat "het sturen en rapporteren over de voortgang en de kwaliteit van de informatiebeveiliging gebeurt op basis van KPI's". Tot nu toe zijn die KPI's niet geformuleerd. In de boardletter 2021 vraagt de accountant aandacht voor de uitwerking hiervan. De gemeenteraad heeft de verantwoording in het kader van ENSIA, inclusief de 'Rapportages Informatiebeveiliging en Privacy' steeds voor kennisgeving aangenomen.

Al met al is de informatiewaarde van de verschillende voortgangs- en verantwoordingsrapportages voor de raad te beperkt om goed invulling te kunnen geven aan zijn controlerende rol.

Behalve de gemeentelijke P&C-cyclus is er ook nog die van de MGR, waar iRvN onder valt. Bij de behandeling van de begroting en jaarstukken van de MGR in de raad wordt niet specifiek over informatiebeveiliging en privacybescherming gesproken. In de bij de MGR ingediende zienswijzen is daar meermaals aandacht voor gevraagd. Daarnaast is in de zienswijzen bij de begroting ingegaan op de invulling van de bezuiniging die iRvN moet doorvoeren. De voortgangsrapportages die de MGR halverwege een jaar aan de gemeenteraad stuurt, zijn door de raad voor kennisgeving aangenomen.

Goede voorbeelden elders

In diverse gemeenten is de afgelopen jaren actief gezocht naar manieren om enerzijds de raad beter te informeren over informatiebeveiliging en privacybescherming, en anderzijds om als raad een actievere rol te spelen in de kaderstelling en controle. Nergens gaat dat zonder problemen, maar we beschrijven enkele voorbeelden waar (kleine) stappen zijn gezet.

- Den Haag: Het college legt de keuze voor de inrichting van de Agenda Digitaal Veilig Den Haag (2022) nadrukkelijk bij de gemeenteraad neer. Het college doet dit, omdat 'het een politieke keuze is of het een kerntaak van de gemeente is om de regie te nemen op de digitale veiligheid van de stad. Het is aan de raad daarover een uitspraak te doen en de inzet en ambitie te bepalen'. Het college helpt de raad bij het maken van die keuze door onder meer drie voorbeeldscenario's uit te werken.
- 's Hertogenbosch: Naar aanleiding van een onderzoek naar informatiebeveiliging heeft de rekenkamer een datawijzer voor de gemeenteraad opgesteld. De datawijzer is een hulpmiddel voor raadsleden om bij raadsvoorstellen waarbij digitale technologie aan de orde is de goede vragen te kunnen stellen en tot een goed afgewogen en onderbouwd besluit te komen.
- Rotterdam: Nadat de Rekenkamer Rotterdam onderzoek had gedaan naar informatiebeveiliging in 2017 heeft het college een Plan van Aanpak opgesteld om tot verbetering te komen. Op basis daarvan heeft de raad extra budget en capaciteit beschikbaar gesteld. Het college heeft de raad vervolgens vier jaar lang elk half jaar geïnformeerd over de voortgang van de uitvoering van het Plan van Aanpak.
- Hilversum: de FG stelt jaarlijks een compact jaarverslag op. De kern hiervan vormen de 'bestuurlijke ontwikkellijn' en de 'ontwikkellijn per aandachtsgebied'. Aan de hand van een compacte set prestatie-indicatoren en met behulp van symbolen wordt voor beide lijnen op één A4 inzichtelijk gemaakt hoe ver

de gemeente is. Daarbij geeft de FG ook steeds een advies. Aan de hand van de scores op de bestuurlijke ontwikkellijn, drukt de FG in één cijfer uit of de sturing op niveau is en, zolang dat nog niet zo is, of er een (voldoende) stijgende lijn te zien in. De gemeenteraad bespreekt het jaarverslag. Het jaarverslag is opgenomen in bijlage 6.

- Amersfoort: in de gemeente Amersfoort wordt een ENSIA-verantwoording van het college aan de raad ontwikkeld, waarin onder andere de stand van zaken voor de verschillende BIO-domeinen en de landelijke voorzieningen, met behulp van indicatoren en symbolen wordt toegelicht. Op dit moment (1 juli 2022) is deze nog niet openbaar.
- Diverse gemeenteraden geven specifiek opdracht aan de accountant om bij zijn jaarlijkse controle aandacht te besteden aan (de voortgang van) de uitvoering van IT-beheersmaatregelen. Zij laten daarover rapporteren in de boardletter en/of laten zich mondeling door de accountant informeren. De gemeenteraden gebruiken deze informatie voor het voeren van gesprekken met het college, maar ook voor het geven van concrete opdrachten om tot verbetering van de informatiebeveiliging te komen. Voorbeelden: gemeente Nijmegen en Provinciale Staten van Gelderland.

Aanbevelingen

14. Stel als raad het beleid voor informatiebeveiliging en privacybescherming vast

Vraag het college om het strategisch beleid voor informatiebeveiliging en privacybescherming ter besluitvorming aan de raad voor te leggen. De raad moet die documenten dan ook agenderen, en de gelegenheid aangrijpen om zich te laten informeren (zie hieronder).

15. Laat je als raad informeren en ondersteunen

Neem als raad zelf het initiatief om je te laten informeren over het belang en de 'basics' van goede informatiebeveiliging en privacybescherming. Doel is om in de daaropvolgende jaren beter te weten waar je op moet letten en naar moet vragen. Nodig het college en ook de CISO en FG voor zo'n sessie uit. Ook een externe deskundige die meedenkt over het soort vragen dat je moet stellen, kan nuttig zijn. Gezien de snelle ontwikkelingen in risico's, dreigingen en techniek, is het verstandig dergelijke sessies met enige regelmaat te organiseren, al dan niet ter voorbereiding op de behandeling van voorstellen of verantwoordingsrapportages die door het college worden voorgelegd. Waarom hier niet een regionaal initiatief van maken?

16. Richt als raad je controlerende rol beter in

Vraag de griffie om in een beknopte nota vast te leggen:

- waarover je als raad wilt worden geïnformeerd: de stand van zaken rond doelen, risico's en maatregelen, de resultaten van testen en toetsen, de toereikendheid van middelen, etc.
- op welke manier je als raad wilt worden geïnformeerd: enkel via de P&C-cyclus, of ook via periodieke informatiebrieven of voortgangsrapportages, via de auditcommissie (desnoods in beslotenheid), etc.
- dat je in ieder geval de jaarlijkse rapportages (ENSIA, privacyjaarverslag) wilt ontvangen en dat die moeten worden voorzien van een begeleidende toelichting. Voor beide rapportages geldt dat daarin inhoudelijk moet worden gerapporteerd op het voldoen aan de vereisten: voor informatiebeveiliging

(ENSIA) zijn dat de BIO-normen en voor privacybescherming de AVG. Verwijs in de nota bijvoorbeeld naar het goede voorbeeld in Hilversum.

- hoe je als raad die informatie agendeert en behandelt, en hoe je de vinger aan de pols houdt. Overweeg om een externe toets of second opinion te vragen, of een adviseur in te schakelen.

17. Overweeg de opdracht aan de accountant voor een IT-audit te continueren

De gemeenteraad is opdrachtgever van de accountant. In de afgelopen raadsperiode was het uitvoeren van een IT-audit onderdeel van die opdracht. Overweeg die opdracht te continueren bij de aanbesteding die in najaar van 2022 aan de orde is voor de jaarrekeningcontrole door de accountant.

18. Overweeg als raden een regionale aanpak

Versterk elkaar als raden en stel bijvoorbeeld een regionale raadswerkgroep in, of gebruik de agendacommissie van de MGR daarvoor. Zo'n gezelschap wordt dan de voorhoede van de gemeenteraden, en de leden ervan houden hun eigen raad goed op de hoogte. Organiseer in die werkgroep de onderlinge uitwisseling en kennisvermeerdering, en stem bijvoorbeeld de controle-activiteiten richting de colleges met elkaar af.

4. REACTIES COLLEGE VAN B&W EN DAGELIJKS BESTUUR MGR

In het kader van hoor- en wederhoor zijn het college en het Dagelijks Bestuur van de Modulaire Gemeenschappelijke Regeling Rijk van Nijmegen in de gelegenheid gesteld te reageren op het rapport, in het bijzonder de aanbevelingen. De reacties zijn opgenomen in dit hoofdstuk.

Reactie College

Geachte heer Backus,

Op 20 mei 2022 heeft u ons het rapport naar aanleiding van het regionale rekenkameronderzoek naar informatiebeveiliging en privacybescherming toegestuurd voor bestuurlijk hoor en wederhoor. Deze brief bevat onze reactie op het voorgelegde rapport.

Inleidend

Ten eerste willen wij onze dank uitspreken voor het werk dat er verzet is in dit onderzoek en de inzichten die het onderzoek oplevert. Zoals u aangeeft is het een omvangrijk onderzoek dat is uitgevoerd op twee complexe en specialistische beleidsterreinen. Deze beleidsterreinen hangen voor een belangrijk deel met elkaar samen maar zijn ook heel verschillend. De uitdagingen op het gebied van informatiebeveiliging en privacybescherming zijn bij gemeenten groot en complex. Met name vanwege de brede taakstellingen binnen het fysiek en sociaal domein die vanuit het rijk de afgelopen jaren richting de gemeente zijn doorgeschoven.

Wij delen met u het belang van het systematisch versterken van de informatiebeveiliging en de bescherming van de privacy van onze inwoners en collega's. Tevens geeft het rapport een realistisch beeld over het volwassenheidsniveau waar de organisatie zich op dit moment bevindt. Dit komt overeen met het volwassenheidsniveau waar veel andere gemeenten zich ook op bevinden en is in onze (gemeentelijke) omgeving geen onbehoorlijke score. We herkennen het nodige van wat er in uw rapport staat en erkennen dat er nog stappen te zetten zijn naar verdere volwassenheid.

In het algemeen

Het is van groot belang dat de inwoners van de gemeente Nijmegen erop kunnen vertrouwen dat hun persoonsgegevens bij ons in veilige handen zijn en dat wij deze persoonsgegevens enkel en veilig verwerken voor het doel waarvoor wij ze ontvangen hebben. Hier moet systematisch op gecontroleerd worden. Daarvoor moeten het college en de gemeenteraad voldoende in positie zijn. Wij onderschrijven daarom grotendeels uw aanbevelingen om de sturing en controle van de gemeenteraad te vergroten. Wij hopen en verwachten dat dit rapport een belangrijke bijdrage zal leveren aan het verder verhogen van het volwassenheidsniveau van onze organisatie. Door de ordening en structuur die het rapport biedt brengt het deze beleidsterreinen op een toegankelijke manier onder de aandacht wat helpt om stappen naar verdere volwassenheid te zetten

Tegelijkertijd heeft het volledig en aantoonbaar in control zijn op het gebied van deze beleidsterreinen een grote impact op de organisatie en de wijze van dienstverlening aan onze inwoners. Hierbij dienen namelijk alle (complexe) processen op papier vastgelegd, vastgesteld, actueel gehouden en aantoonbaar gemonitord te worden. Dit zal een belangrijke investering vragen in tijd en geld bovenop de investeringen die we al gedaan hebben om het huidige niveau te behalen. Dit in een tijdsperiode waarin veel urgente taken van de Rijksoverheid naar de gemeenten zijn gedecentraliseerd die ook de nodige middelen vragen.

Hieronder geven wij onze reactie op de verschillende aanbevelingen.

Informatiebeveiliging en privacybescherming

1. Zorg voor heldere afspraken tussen de gemeenten en iRvN over informatiebeveiliging
We delen deze aanbeveling. Om deze reden zijn we in 2021 met iRvN begonnen te werken met resultaatverwachtingen die te verantwoorden zijn. We zijn een resultatenmatrix aan het opbouwen, die leidt tot scherpere afspraken in de volgende actualisatie van de afsprakenkaders die wij met iRvN hebben. Daarin leggen wij vast welke acties met welk kwaliteitsniveau wij op welk moment van elkaar verwachten en hoe wij op die afspraken reflecteren. Een andere manier waarop we onze afspraken met iRvN zullen verduidelijken is door de uitvoering van, en verantwoordelijkheid over informatiebeveiligingsmaatregelen te expliciteren.

2. Overweeg om het pad in te slaan van gezamenlijk informatiebeveiligingsbeleid in de regio
In de aanbeveling zitten waardevolle opmerkingen over verdere doorgroeimogelijkheden van het volwassenheidsniveau. Gedurende de doorlooptijd van het Rekenkameronderzoek is ook het evaluatierapport naar de ICT-functie in de iRvN -regio afgerond en vastgesteld. iRvN heeft en houdt de opdracht om verantwoordelijk te zijn voor de technische aspecten van informatiebeveiliging. De gemeenten zijn verantwoordelijk voor de inhoudelijke, beleids- en procesmatige aspecten ervan en stellen het informatiebeveiligingsbeleid autonoom vast. Het rekenkameronderzoek wijst op de overlap (of ‘het grijze gebied’) tussen beide. De oproep is nadrukkelijk gehoord en wordt vertaald in nadere samenwerkingsafspraken tussen de gemeenten onderling en met iRvN waarmee de samenwerking door kan groeien op inhoudelijke thema’s. Zoals het verloop van dit rekenkameronderzoek ook laat zien kost regionale samenwerking tijd. Alleen ga je vaak sneller, maar samen kom je verder. Waar de meerwaarde van samenwerking op weegt tegen de doorlooptijd die zij vraagt zullen wij deze extra tijd zeker investeren.

3. Verhelder het beleid voor informatiebeveiliging en privacybescherming
Deze aanbeveling onderschrijven wij. Wij zullen middels een update van het strategische privacybeleid in Q4 van dit jaar uitvoering geven aan deze aanbeveling. Het informatiebeveiligingsbeleid is in 2022 herzien. In de komende herziening zullen wij volgens afspraak het genoemde strategische beleid evalueren met de auditcommissie.

4. Werk zo snel mogelijk de belangrijkste ontbrekende onderdelen van het beleid uit
Deze aanbeveling omarmen wij, met de kanttekeningen dat wij onze verantwoordelijkheid moeten bezien binnen onze reële mogelijkheden en ambtelijke capaciteit, gelet op de complexiteit van informatiebeveiliging en privacybescherming. Hierbij onderschrijven wij de urgentie van de uitdagingen vanuit privacybescherming op dit beleidsterrein. Wij zullen ook met partners binnen het sociaal domein onderzoeken hoe we privacybescherming structureel verder kunnen versterken.

Vanuit de kaders van het informatiebeveiligingsbeleid wordt op een aantal deelgebieden nog nader beleid ontwikkeld. Dit gebeurt op regionaal niveau. Op een aantal onderdelen zijn op deze manier beleidsvoorstellen in de regio uitgewerkt en vastgesteld.

5. Voer zo snel mogelijk een organisatie brede risicoanalyse uit
Deze aanbeveling nemen wij over. In Q3 en Q4 zullen wij een analyse door een externe partij laten uitvoeren.

6. Maak risicomanagement tot een continu proces
De aanbeveling tot het inrichten van een continu proces op risicobeheersing nemen wij over. Hiervoor is onder andere de applicatie CyberManager aangeschaft die inzicht verschaft op risicobeheersing op het vlak van informatiebeveiliging. Wij zien dit als een zeer waardevol sturingsinstrument om de betrokkenheid van de organisatie en de raad te vergroten.

Het cyclisch proces op privacybescherming is meegenomen bij de uitvoering van de controle door de Functionaris voor de gegevensbescherming in 2021 op de uitvoering van privacy analyses en verwerkersovereenkomsten. Dit proces zal verder uitgewerkt moeten worden zodat het werken volgens processen en protocollen met bewijsstukken aangetoond kan worden.

Het risicomanagement proces zal onderdeel zijn van het vaste auditproces waarin de Auditcommissie betrokken is namens de raad.

7 en 8. Stel voldoende (financiële) middelen beschikbaar, geef de CISO en FG de beschikking over een eigen budget
Het college neemt deze aanbevelingen ter harte en wil met de raad in gesprek over de benodigde financiële middelen. Bij het volwassenheidsniveau waar wij als gemeente naar streven horen investeringen. We komen met een uitwerking in scenario's behorend bij deze investeringen. Deze vormen samen een risicobeheersingsplan dat leidt naar een voldoende niveau van beveiliging en bescherming zoals bepaald door de raad. Binnen het totale budget voor informatiebeveiliging en privacybescherming zal ook ruimte toegewezen moeten worden aan de CISO en FG functies. Hierbij willen wij benadrukken dat er meer bemensing nodig is dan enkel de CISO en de FG. Gevraagde extra audits en analyses, deskundigheidsbevordering, extern advies, bevordering van het bewustzijn in de organisatie en geautomatiseerde ondersteuning zijn mogelijke activiteiten die met een gereserveerd budget met meer slagkracht kunnen worden uitgevoerd.

9. Leg vast hoe je gaat toetsen en rapporteren
Uw rekenkamer benoemt een aantal concrete punten c.q. voorbeelden van andere gemeenten op het gebied van toetsingscriteria en bijbehorende indicatoren als ook het periodiek informeren van de raad via rapportages en besprekingen. Op dit moment kunnen wij nog niet geheel overzien welke impact de door u gestelde inhoudelijke verantwoording heeft op de gemeentelijke organisatie. Het uitgangspunt zal zijn dat alle afdelingen moeten toetsen en rapporteren. De aanbeveling om dat in te richten nemen wij dan ook over. Om dit zo efficiënt mogelijk te doen willen we hiervoor zoveel mogelijk aansluiten op de bestaande P&C cyclus. Tegelijkertijd zal de realisatie hiervan om een investering vragen omdat de verantwoordingsactiviteiten passend bij een hoger volwassenheidsniveau, misschien deels geautomatiseerd, ook door medewerkers uitgevoerd zullen moeten worden.

10. Ga KPI's gebruiken
Deze aanbeveling nemen wij ter harte. In de actualisatie van het privacy beleid zullen wij aandacht besteden aan meetbare resultaten aan de hand van het borgingsproduct van de Informatiebeveiligingsdienst (IBD). In samenwerking met iRvN zijn wij op het gebied van informatiebeveiliging begonnen met het opbouwen van KPI's.

11. Zet volop en systematisch in op bewustwording
Deze aanbeveling wordt geïmplementeerd door onder andere de verplichte deelname van alle medewerkers aan de e-Learning campagne. Tevens hebben we regelmatig i-Bewustwordingscampagnes en maatwerktrajecten binnen de verschillende afdelingen. Daarnaast onderzoeken wij hoe systematisch invulling te geven aan bewustwording op deze beleidsterreinen. Alle afdelingen kennen privacy ambassadeurs die tot taak hebben het bewustzijn in de afdeling op deze terreinen te bevorderen door collega`s te ondersteunen bij het maken van de juiste keuzes. Vanaf eind 2022 kunnen we deze ontwikkeling structureel volgen en daarmee continu bijsturen.

12 en 13. Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming in de gemeente en de regio
Wij horen uw oproep maar herkennen onszelf niet in de conclusie dat er in Nijmegen te weinig bestuurlijke aandacht is voor deze onderwerpen. Het college heeft de raad diverse keren per jaar over de voortgang van het informatiebeleid geïnformeerd en het onderwerp besproken via het auditoverleg in de auditcommissie. In Nijmegen wordt het jaarverslag van de Functionaris voor de gegevensbescherming (FG) alsook de Rapportage informatiebeveiliging en privacy aangeboden aan het college als onderdeel van de ENSIA verantwoording. Meer en gerichte bestuurlijke aandacht van de raad kan helpen om tot betere prioritering te komen, zeker als het gaat om het vaststellen van beleid alsmede de bijbehorende financiële kaders. Het agenderen van deze thema`s en het ambtelijk verzorgen van een toelichting hier over is altijd mogelijk.

Rol van de raad

Over de rol van de raad zijn de volgende aanbevelingen opgenomen in het rapport:

- 14. Stel het beleid voor informatiebeveiliging en privacybescherming vast
- 15. Laat je informeren en ondersteunen
- 16. Richt je controlerende rol beter in
- 17. Overweeg de opdracht aan de accountant voor een IT-audit te continueren
- 18. Overweeg een regionale aanpak

De begeleiding door de accountant heeft de afgelopen jaren vruchten afgeworpen. De raad is in de afgelopen jaren regelmatig geïnformeerd over de voortgang op het terrein van iVeiligheid. Met name via de audit commissie maar ook via stukken die aan de raad zijn verstrekt, zoals het jaarverslag. Wij willen de raad adviseren aan de hand van deze informatie het gesprek aan te gaan en zich, als daar behoefte aan is, meer uitgebreid te laten voorlichten over dit onderwerp. Dit kan bijvoorbeeld door de betreffende functionarissen uit te nodigen.

Gezien de raad over haar eigen rol gaat, wachten wij voorstellen van de raad en griffie hieromtrent met belangstelling af.

Hoogachtend,
het college van burgemeester en wethouders van Nijmegen

mr. drs. A.H. van Hout	drs. H.M.F. Bruls
gemeentesecretaris	burgemeester

Reactie Dagelijks Bestuur MGR Rijk van Nijmegen

Beste leden van de Regionale Rekenkamers,

Op 20 mei jl. hebben wij het rapport ‘Weten wat je moet weten’ van u ontvangen. Aanleiding van het rapport is het onderzoek naar informatiebeveiliging en privacybescherming binnen het ICT-samenwerkingsverband. U heeft ons om een reactie op het rapport gevraagd. Hierbij vindt u onze reactie ten aanzien van de onderdelen in het rapport, die betrekking hebben op de module iRvN van de MGR.

Binnen het ICT-samenwerkingsverband is de module iRvN van de MGR een uitvoeringsorganisatie voor alles wat te maken heeft met het beheer en de zo veilig mogelijke verwerking van gemeentelijke gegevens binnen een gedeelde regionale infrastructuur. iRvN doet dit op één manier die voor alle deelnemende gemeenten van de MGR hetzelfde is.

In uw rapport doet u - in paragraaf 3.2 ‘Weten wie wat doet: taakafbakening en afspraken gemeenten-iRvN’ en paragraaf 3.8 ‘Weten dat je verantwoordelijk bent: bestuurlijke verantwoordelijkheid en commitment’ – aanbevelingen, richting iRvN. Wij nemen deze aanbevelingen ter harte.

In paragraaf 3.2 gaat het om de aanbevelingen:

1. *Zorg voor heldere afspraken tussen de gemeenten en iRvN over informatiebeveiliging*
   a. Dit voorkomt risico’s als gevolg van onduidelijkheid hierover, en stelt iRvN in staat de gemeenten beter en efficiënter te ondersteunen. Vraag het college over een jaar te rapporteren, liefst op basis van een extern onderzoek.
   b. Vraag het college om in MGR-verband een meerjarenbeleidsplan voor de ICT-module op te stellen met daarin duidelijke doelstellingen. Vraag het college dit beleidsplan op hoofdlijnen uit te werken in een (meerjaren)uitvoeringsprogramma, waarin wordt ingegaan op de benodigde inspanningen door zowel iRvN

als de gemeenten. Bijzondere aandacht verdient daarbij het opstellen van de tot nu toe ontbrekende (beleids)kaders voor informatiebeveiliging. Overweeg als raad de zienswijzen op dit meerjarenbeleidsplan gezamenlijk met de andere raden voor te bereiden.

c. Vraag het college om het dagelijks bestuur van de MGR voortaan, op basis van het meerjarenbeleidsplan en – uitvoeringsprogramma, een jaarlijks uitvoeringsprogramma (collectieve DVO) vast te laten stellen. Vraag het college om het dagelijks bestuur in de jaarstukken verantwoording af te laten leggen over de doelstellingen.

Reactie: Een heldere set van afspraken en ICT-doelstellingen ondersteunt iRvN bij een goede uitvoering van de opdracht van de deelnemende gemeenten op het gebied van Informatiebeveiliging en privacybescherming. Op basis van een gemeentelijk meerjarenbeleidsplan en -uitvoeringsprogramma zijn we in staat om een jaarlijks uitvoeringsprogramma te realiseren. Ons inziens is het noodzakelijk dat we hier spreken van een – zo maximaal op elkaar afgestemd - regionaal beleidsplan en -uitvoeringsprogramma. Voor iRvN is het nl. belangrijk dat de uitvoeringspraktijk voor alle deelnemende gemeenten gelijkwaardig kan en mag zijn. Op deze manier kan iRvN de ondersteuning effectief en efficiënt organiseren.

2. *Overweeg om het pad in te slaan van gezamenlijk informatiebeveiligingsbeleid in de regio*.
   Vraag het college om bestuurlijk de discussie aan te gaan om toch tot een gezamenlijk informatiebeveiligingsbeleid in de regio te komen. Voor de hand ligt om iRvN daarvoor te gebruiken: de organisatie staat al, en is bestuurlijk ingebed in de MGR. Een gezamenlijk beleid, waarin onder meer is vastgelegd welk gedeeld volwassenheidsniveau de gemeenten nastreven, is de beste manier om de informatiebeveiliging in onze gemeenten te vergroten en de risico's te verminderen. Laat je als raad informeren over de mogelijke keuzes en implicaties daarvan. Bij het bepalen van je standpunt hierover kun je je als gemeenteraad extern laten adviseren. Overweeg dat in regionaal verband te doen.

Reactie: bij informatiebeveiliging gaat het om de beveiliging van gegevens en systemen: het ervoor zorgen dat de aanwezigheid en beschikbaarheid van gegevens en systemen gewaarborgd is en gegarandeerd is volgens wet- en regelgeving, zoals de Baseline Informatiebeveiliging Overhead (BIO) en de Algemene verordening privacywetgeving (AVG). Bij beveiligingsmaatregelen gaat het er om dat de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau beperkt wordt. Om dit niveau te bepalen toetst iRvN nieuwe applicaties aan de BIO en AVG.
De informatiebeveiliging is een verantwoordelijkheid van de gemeente zelf. iRvN heeft en houdt de opdracht verantwoordelijkheid te dragen voor de technische aspecten van informatiebeveiliging. De gemeenten zijn verantwoordelijk voor de inhoudelijke, beleids- en procesmatige aspecten ervan. In het rapport wordt melding gemaakt van het risico op overlap (of 'het grijze gebied') tussen beide. De oproep tot afstemming c.q. duidelijkheid over de verantwoordelijkheden is nadrukkelijk gehoord en wordt vertaald in nadere samenwerkingsafspraken tussen de gemeenten onderling en met iRvN.
Eén allesomvattend regionaal Informatiebeveiligingsbeleid is een uitdagende ambitie. Voor iRvN is het van belang dat er een regionaal beleid wordt geformuleerd, voor die onderdelen die zijn uitbesteed aan iRvN, waarbij de standaardproducten van de BIO, de Informatiebeveiligingsdienst (IBD) en Vereniging Nederlandse Gemeenten (VNG) als uitgangspunt dienen.

iRvN biedt graag haar kennis en ondersteuning aan om te komen tot meer stappen richting een gezamenlijk regionaal informatiebeveiligingsbeleid. Het regionaal informatiebeveiligingsbeleid vormt de basis voor de 'Basisafspraken ICT-diensten', waarin de dienstverlening van iRvN aan alle deelnemende gemeenten is vastgesteld. De Basisafspraken worden ook wel de 'collectieve dienstverleningsovereenkomst' genoemd. Onderdeel van deze Basisafspraken is een productencatalogus. Daarin is uitgewerkt welke producten en diensten iRvN levert en welke daarvan verplicht of optioneel door de gemeenten worden afgenomen.

Wij zullen – in overleg met de deelnemende gemeenten – zorgdragen voor herijking van de Basisafspraken, op grond van het nieuwe (regionaal) informatiebeveiligingsbeleid.

In paragraaf 3.8 gaat het om de aanbevelingen:

1. *Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming in de gemeente.*
   Vraag het college – in lijn met VNG-resolutie 2021 en de 10 bestuurlijke principes voor informatiebeveiliging - om de portefeuilles informatiebeveiliging en privacybescherming voldoende gewicht te geven en systematisch aandacht te besteden in de collegevergaderingen aan zaken zoals risico's, beleid, prioritering, benodigde middelen, jaarplannen, monitoring, voortgangs- en verantwoordingsrapportages en de eigen bewustwording.

2. *Besteed meer bestuurlijke aandacht aan informatiebeveiliging en privacybescherming in de regio Versterk en verduidelijk de governance op regionaal niveau.*
   Vraag het college om in MGR-verband voldoende gewicht te geven aan de rol van IRvN bij de informatiebeveiliging in de gemeenten (en bij iRvN zelf). Dat betekent periodieke aandacht in het Algemeen Bestuur en in de Agendacommissie van de MGR voor informatiebeveiliging, zowel als het gaat om beleidsplan en jaarplannen (Plan) en rapportages (Check). Ook (of: juist) als de aansturing van iRvN bij de gemeentesecretarissen en/of hoofden bedrijfsvoering ligt, zorg dan voor noodzakelijke bestuurlijke besluitvorming in het AB. Vraag aan het college om de instelling van een aparte bestuurscommissie voor iRvN in het AB van de MGR te overwegen.

Reactie op beide aanbevelingen: wij ondersteunen deze aanbevelingen. Binnen ons bestuur van de MGR maken wij afspraken over een jaarlijks op te stellen uitvoeringsprogramma Informatiebeveiliging (inclusief de Basisafspraken c.q. collectieve DVO), een adequate wijze van monitoring van dit uitvoeringsprogramma en de genomen maatregelen in het kader van privacybescherming. Hierbij betrekken wij de agendacommissie van de MGR.

Wij hopen u hiermee voldoende geïnformeerd te hebben,

Hoogachtend,

Dagelijks Bestuur modulaire gemeenschappelijke regeling Rijk van Nijmegen,

De voorzitter, De secretaris,

Drs. H.M.F. Bruls J. Hol

5. NAWOORD REKENKAMER(COMMISSIE)S

De samenwerkende rekenkamer(commissie)s willen hun tevredenheid uitspreken over de bestuurlijke reacties van de colleges van B&W van Berg en Dal, Beuningen en Nijmegen, en die van het DB van de MGR Rijk van Nijmegen. De reactie vanuit Wijchen is op dit moment (1 juli 2022) nog niet beschikbaar.

Uit de bestuurlijke reacties spreekt in grote lijnen herkenning van de uitkomsten en instemming met de aanbevelingen. Het is goed om te lezen dat er de afgelopen maanden al diverse zaken in gang zijn gezet, en dat er ook de komende tijd op veel punten stappen zullen worden gezet in onze gemeenten. We zijn blij dat het rekenkamerrapport daarbij als bruikbaar wordt beschouwd. Wij adviseren onze gemeenteraden om de plannen en uitvoering door hun college actief te volgen de komende tijd, in lijn met de vijf aanbevelingen aan de raad.