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

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.

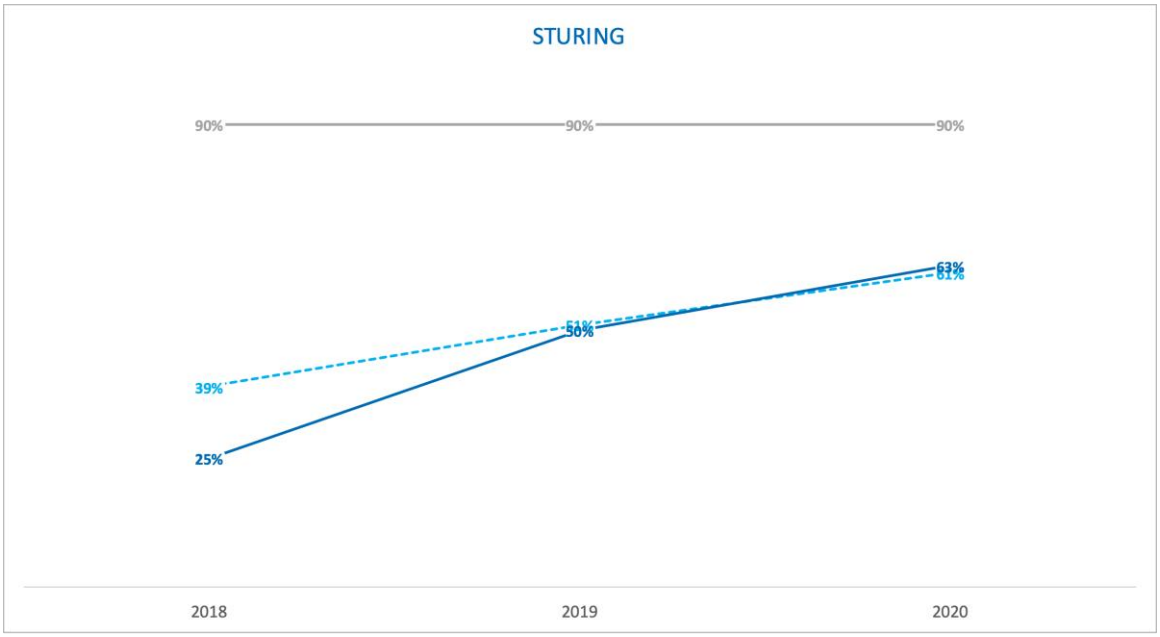
[2] Artikel 1 AVG - waarbij aangetekend dat het niet alleen gaat om bescherming van de persoon in kwestie maar ook om de bescherming van anderen zoals bijvoorbeeld omwonenden.

[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.