Onderzoek naar Informatiebeveiliging & bescherming van persoonsgegevens gemeente Roermond

Rekenkamercommissie Roermond
April 2018

Rekenkamercommissie
Gemeente Roermond
Postbus 900
6040 AX Roermond

Colofon

Samenstelling Rekenkamercommissie

Externe leden
De heer mr. P.M.B. Schrijvers (voorzitter)
De heer ir. N. op de Laak

Raadsleden
Mevrouw L. van Hal
De heer C.W.A. Achten
De heer J.M.W. de Kunder

Secretariaat Rekenkamercommissie

Ambtelijk secretaris
De heer A.H.C. Vestjens

Adres
Postbus 900

Telefoonnummer
0475 – 35 94 60

E-mail
arnovestjens@roermond.nl

Website
www.roermond.nl

April 2018

Inhoudsopgave:

Bijlagen:

1. Doelstelling en vraagstelling.

De Rekenkamercommissie (RKC) heeft op 12 september 2017 de gemeenteraad en het college van B&W geïnformeerd over de start van het onderzoek Informatiebeveiliging & bescherming van persoonsgegevens.

Doelstelling van het onderzoek:
Het doel is om na te gaan op welke wijze(n) de gemeente Roermond informatieveiligheid heeft georganiseerd en hoe in dat verband de werkprocessen daarop reeds zijn ingericht en hoe de bescherming van persoonsgegevens geborgd is.

Vraagstelling van het onderzoek:

1. Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?
2. Hoe geeft de gemeente Roermond vorm en inhoud aan het informatieveiligheidsbeleid?
3. Heeft de gemeente voldoende adequate maatregelen getroffen om de persoonsgegevens die zij in beheer heeft, te beschermen tegen de belangrijkste veiligheidsrisico's?

3a. Wat is de samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op samenwerking met derden en informatie-uitwisseling?

4. Hoe is de communicatie / afstemming / sturing met betrekking tot het informatieveiligheidsbeleid tussen het college van B&W (college) en de ambtelijke organisatie geregeld?
5. Hoe is / wordt de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid vorm en inhoud gegeven?

2. Onderzoeksaanpak en -fasering.

Om tot de beantwoording van de onderzoeksvraag en -deelvragen te komen, is als volgt te werk gegaan.

De RKC heeft (op grond van een onderhandse aanbestedingsprocedure) het onderzoek uitbesteed aan bureau Berenschot.

Samen met de onderzoekers van Berenschot heeft de RKC bij aanvang van het onderzoek een startbijeenkomst georganiseerd met de portefeuillehouder en medewerkers uit de ambtelijke organisatie die bij het onderzoek zouden worden betrokken.

De RKC heeft Berenschot gevraagd het onderzoek uit te voeren, aan de hand van de vraagstelling en op basis van een door de RKC vastgesteld normenkader (zie het onderzoeksrapport van Berenschot, paragraaf 3.2., voor het gehanteerde beoordelingskader).

Vervolgens hebben de onderzoekers een documentenstudie uitgevoerd. De bevindingen uit de documentenstudie zijn met behulp van de interviews getoetst. Er zijn interviews gehouden met onder meer (een afvaardiging van) de gemeenteraad, het college van b en w, griffier, gemeentesecretaris, diverse afdelingshoofden en medewerkers en enkele externe partijen. Daarnaast zijn er twee case studies uitgevoerd. Een case studie ‘totstandkoming van informatiebeveiligingsbeleid’ en een case studie met betrekking tot het Zorgteam.

Daarna is de conceptrapportage aan de RKC voorgelegd. Deze rapportage (d.w.z. het rapport met het feitenrelaas, zonder aanbevelingen) is vervolgens op 29 januari 2018 toegestuurd aan de ambtelijke organisatie voor een controle op de juistheid van de feiten.

Naar aanleiding daarvan is het rapport (qua beschrijving van de feiten) op enkele punten aangepast en heeft de RKC de aanbevelingen vastgesteld.

Op 10 april 2018 is de rapportage (met de aanbevelingen) voorgelegd aan het college van B&W voor een bestuurlijke reactie.

De reactie van het college en het nawoord van de RKC zijn opgenomen in bijlage I.

3. Conclusie, beantwoording onderzoeksvragen en aanbevelingen.

De algemene conclusie naar aanleiding van het onderzoek en de beantwoording van de onderzoeksvragen (zoals verwoord in paragraaf 4.1. en 4.2. van het bijgevoegde rapport van Berenschot) treft u onderstaand integraal aan. De RKC heeft op basis daarvan haar aanbevelingen geformuleerd.

Algemene conclusie.

Uit het onderzoek komt het algemene beeld naar voren dat de gemeente Roermond de informatiebeveiliging en bescherming van persoonsgegevens goed heeft geregeld en dat vanuit de ambtelijke organisatie, met name vanuit de CISO, senior adviseur privacy/privacy officer en de gemeentesecretaris, de borging degelijk is. Wat verder opvalt, is dat de borging van deze twee thema's steeds zwakker wordt hoe meer men 'boven in de organisatie' terechtkomt, met name bij de gemeenteraad en het college. De gemeenteraad en het college staan op behoorlijke afstand van deze thema's, maar zij hebben wel vertrouwen in de ambtelijke organisatie dat zij goed omgaan met informatiebeveiliging en de bescherming van de persoonsgegevens en dat de ambtelijke organisatie het ook goed regelt.

De proactieve inzet van een klein aantal belangrijke functionarissen, te weten de CISO, senior adviseur privacy, privacy officer en de gemeentesecretaris, in afstemming met de portefeuillehouder, zorgt voor een inhoudelijke kruisbestuiving die op het gebied van informatiebeveiliging en bescherming van persoonsgegevens al jaren zijn vruchten afwerpt richting de gemeentelijke organisatie. Aan de huidige kleine bezetting van één CISO, senior adviseur privacy en privacy officer, de beperkte achtervang voor deze senior functionarissen en samenballing van deskundigheid binnen dit team kleven de risico's dat, mede vanwege de leeftijdsopbouw, zowel de opvolging als de continuïteit van dit team op korte termijn kwetsbaar zijn.

Aandacht binnen de ambtelijke organisatie van de gemeente Roermond voor de thema's informatiebeveiliging en bescherming van persoonsgegevens blijft echter wel vereist en dit geldt ook voor het college en de raad. Naast een hoge mate van bewustzijn binnen de ambtelijke organisatie worden de thema's informatiebeveiliging en bescherming van persoonsgegevens ook geladen vanuit andere thema's als integriteit en de eigen professionaliteit bij het uitvoeren van werkzaamheden.

Uit de eerste case studie met betrekking tot de totstandkoming van het informatiebeveiligingsbeleid volgt dat de ontwikkeling van het thema informatiebeveiliging verder in de volwassenheidscyclus terecht gekomen is en dat daarmee de fase van opstarten en pionieren afgesloten is. Het beleid is tot stand gekomen door de focus, vastberadenheid en inzet van een klein team mensen. De communicatie en afstemming in het kader van de totstandkoming van het informatiebeveiligingsbeleid is vanuit de ambtelijke organisatie op een gestructureerde wijze uitgevoerd.

Uit de tweede case studie inzake het Zorgteam is gebleken dat er een grote mate van aandacht en bewustzijn is met betrekking tot het thema privacy en het delen van gegevens. Eén van de zorgen is echter dat dit thema in het algemeen mogelijk ten koste kan gaan van doelmatigheid, de werkbaarheid voor medewerkers en dienstverlening aan burgers. Dit aandachtspunt geldt specifiek voor het gemeentelijke sociaal domein waarin integraal werken over de beleidsvelden heen de wens is, maar het als lastig wordt ervaren om gegevens te delen.

Beantwoording onderzoeksvragen.

1. Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?

De gemeente Roermond heeft in brede zin een goed beeld van de risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens.

De bewustwording van informatiebeveiliging en bescherming van persoonsgegevens is vanaf 2005 binnen de ambtelijke organisatie gegroeid. Bij het college en de raad leven de thema's informatiebeveiliging en bescherming van persoonsgegevens wel, maar staan op een vrij hoog abstractieniveau. Binnen het college is de portefeuillehouder gepositioneerd om het college te informeren over de thema's. De raad staat op afstand van de thema's en heeft onvoldoende inzicht in de risico's.

In het informatiebeveiligingsplan, Jaarplan Informatiebeveiliging en privacybeleid wordt duiding gegeven aan de risico's die gezien worden. In meer operationele zin is het uitvoeren van risicoanalyses opgenomen in het actuele beveiligingsbeleid en wordt dit toegepast in de praktijk, bijvoorbeeld door het uitvoeren van baseline toetsen en privacy impact analyses. In de periode juni 2015 t/m oktober 2017 zijn bijvoorbeeld 11 baseline toetsen uitgevoerd binnen de gemeente Roermond. Mede op basis van baselinetoetsen zijn specifieke aanvullende risicoanalyses en privacy impact analyses uitgevoerd en zijn specifieke aandachtsgebieden terugvertaald in het Jaarplan Informatiebeveiliging.

2. Hoe geeft de gemeente Roermond vorm en inhoud aan het informatieveiligheidsbeleid?

Het informatiebeveiligingsbeleid is vanaf 2005 regelmatig (her)beoordeeld, gewijzigd en opnieuw vastgesteld door de betrokken actoren in de organisatie (CISO, senior adviseur privacy, MT en college). De taken, bevoegdheden en verantwoordelijkheden zijn duidelijk beschreven in het beleid. De wijzigingen van het beleid zijn besproken in de werkgroep, projectgroep en uiteindelijk stuurgroep informatiebeveiliging & privacy. Het informatiebeveiligingsbeleid is voor iedereen terug te vinden op het gemeentelijke intranet.

Het informatieveiligheidsbeleid en het Jaarplan Informatiebeveiliging zijn gebaseerd op de baseline informatiebeveiliging gemeente (BIG). Met behulp van de GAP-analyse worden acties geprioriteerd. Het informatiebeveiligingsbeleid bevat inzicht in risico's en is ingericht op het mitigeren van deze risico's. Naast de formele documenten is op basis van de gesprekken een hoge mate van bewustwording geconstateerd met betrekking tot informatiebeveiliging en privacy.

3. Heeft de gemeente voldoende adequate maatregelen getroffen om de persoonsgegevens die zij in beheer heeft, te beschermen tegen de belangrijkste veiligheidsrisico's?

De gemeente heeft maatregelen getroffen om de persoonsgegevens die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's. Het betreft maatregelen op het gebied van personele beveiliging, bedieningsprocessen, verwerving van systemen en naleving van wet- en regelgeving. In het Jaarplan Informatiebeveiliging 2017 zijn diverse maatregelen opgenomen in de gevallen dat de eigen norm met betrekking tot personele beveiliging en verwerving van systemen net niet zijn behaald. Het beheer van bedieningsprocessen blijft met de score op het zelf assessment net iets achter op de gewenste score. Opvallend is dat er geen directe punten voor verbetering zijn opgenomen in het Jaarplan Informatiebeveiliging 2017.

3a. Wat is de samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op de samenwerking met derden en informatie-uitwisseling?

Op basis van de documentatie en gesprekken is een lijn zichtbaar dat medewerkers zeer bedacht zijn bij de informatie-uitwisseling, zowel intern als in de relatie met derden. Er is een hoge mate van bewustwording en bewustzijn op het gebied van informatiebeveiliging en privacy en het besef dat het bij uitstek gaat om gevoelige informatie. In de werkprocessen wordt rekening hiermee gehouden door bijvoorbeeld met kopieën te werken waarin object gebonden in plaats van persoonsgebonden informatie is opgenomen. Bij de afdeling Publiekszaken is een effect beschreven dat er een spagaat wordt ervaren tussen wat mag en wat relevant is voor de klant en dat deze lijn in de praktijk lastig is te trekken en dat hierdoor de dienstverlening aan burgers kan worden geraakt.

4. Hoe is de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie geregeld?

Er is periodiek overleg binnen de werkgroep-, adviesgroep- en stuurgroep informatiebeveiliging & privacy. In deze overleggen zijn de operationele, tactische en strategische vraagstukken belegd en helder beschreven in het informatiebeveiligingsbeleid. Het college neemt geen actieve rol in bij de totstandkoming van het beleid en heeft een grote mate van vertrouwen in de ambtelijke organisatie en dat zij het goed regelen. Een markant punt is dat het college recentelijk het informatiebeveiligingsbeleid aangenomen heeft zonder inhoudelijke discussie, terwijl het college ook aangeeft dat deze materie voor hen vrij abstract is. De interne communicatie over incidenten of calamiteiten loopt in eerste instantie via de gemeentesecretaris en de portefeuillehouder en bij ernstige incidenten worden het college en de raad geïnformeerd.

5. Hoe is de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid en privacy vorm en inhoud is/wordt gegeven?

Een raadsdelegatie die de onderzoekers gesproken heeft, geeft te kennen dat informatieveiligheid en privacy vrij technische materie betreft die een hoge dosis van expertise verlangt, hetgeen in de raad maar mondjesmaat aanwezig is. De bewustwording binnen de raad is naar eigen zeggen nog in een beginstadium en groeiende, maar in beperkte mate. Vanuit de raadsdelegatie is aangegeven dat het daardoor lastig is kaders te stellen. Zonder gestelde kaders is het adequaat invulling geven aan de controlerende taak (toetsen aan de kaders) niet mogelijk.

Er zijn door de raad geen specifieke spelregels vastgelegd over hoe de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de thema's informatiebeveiliging en privacy vorm en inhoud is/wordt gegeven. De raad heeft geen specifieke informatiebehoefte aangegeven aan het

college met betrekking tot informatiebeveiliging en privacy waardoor er geen kaders zijn die SMART / meetbaar geformuleerd zijn. Door het college wordt op verzoek van de raad voldaan aan de informatieplicht, zij het dat de raad ad hoc vragen heeft gesteld. De controle en bijsturing van de raad is echter nihil en er is daardoor geen sprake van het realiseren of heroverwegen van doelstellingen. Het thema informatiebeveiliging en privacy wordt nauwelijks geagendeerd in de raad dan wel commissie.

In de regeling van het Auditcomité is sinds medio 2016 opgenomen dat het Auditcomité als taak heeft het voeren van overleg met het college van B&W over informatieveiligheid, maar dit is echter niet specifiek ingestoken vanuit de raad zelf. Aan het Auditcomité worden diverse rol- en taakinvullingen toegedicht. Deze diversiteit aan visies draagt nog niet adequaat bij aan de kaderstellende rol van de raad. Vanuit de raad of commissie wordt het Auditcomité nog niet aangesproken of aangestuurd om informatiebeveiliging en privacy op de agenda te zetten. Pas in juni 2017 is in het Auditcomité een presentatie over ENSIA en over Privacy (Wbp en AVG) gegeven en in december 2017 zijn informatiebeveiliging en privacy weer geagendeerd; dit overleg is in afstemming met de portefeuillehouder georganiseerd. De rol van het Auditcomité op het gebied van informatiebeveiliging en privacy is nog nieuw en nog niet uitgekristalliseerd.

Aanbevelingen

De volgende aanbevelingen zijn vastgesteld door de RKC naar aanleiding van het onderzoek:

Gemeenteraad

- Maak als gemeenteraad zo snel mogelijk een start, mede gelet op inwerkingtreding van de AVG per 25 mei 2018, met het stellen van kaders met betrekking tot informatiebeveiliging en bescherming van persoonsgegevens zodat men als gemeenteraad in stelling komt om te controleren en (bij) te sturen, overleg hierover met het college waarbij er aandacht is voor het SMART formuleren van de kaders bijvoorbeeld met betrekking tot risico's en kwetsbaarheden, maatregelen en middelen die bijdragen aan de continuïteit van dienstverlening en een prioriteitenstelling.
- Bepaal als gemeenteraad welke informatievoorziening benodigd is, bijvoorbeeld door bij raadsvoorstellen de onderwerpen informatieveiligheid en bescherming van persoonsgegevens expliciet op te nemen in het format van raadsvoorstellen, en stem de spelregels over de informatievoorziening en verantwoording af met het college.
- Ga met het college halfjaarlijks de discussie aan over informatiebeveiliging en bescherming van persoonsgegevens zodat de gezamenlijke 'sense of urgency' gevoed blijft.
- Leg expliciet vast hoe de informatievoorziening jaarlijks vanuit het Auditcomité richting de gemeenteraad gebeurt.
- Maak meer gebruik van het Auditcomité door informatiebeveiliging en bescherming van persoonsgegevens te (laten) agenderen en evalueer tweejaarlijks de rolinvulling van het Auditcomité ten aanzien van deze twee thema's c.q. heroverweeg dit zo nodig.

College

- Wees als college aanjager van de thema's informatiebeveiliging en bescherming van persoonsgegevens door deze thema's aan de vakgebieden van medewerkers te verbinden waardoor er continu communicatie, aandacht en bewustwording is voor deze thema's. Betrek medewerkers bijvoorbeeld door jaarlijkse presentaties of workshops over informatiebeveiliging en bescherming van persoonsgegevens te organiseren.

- Ga halfjaarlijks de discussie aan met de raad over de thema's informatiebeveiliging en bescherming van persoonsgegevens, bijvoorbeeld over de prioriteitenstelling van te nemen maatregelen in het kader van de AVG.
- Leg nog meer en expliciet vast met betrekking tot de werkprocessen en procedures behorend bij informatiebeveiliging en privacy waardoor er voor medewerkers vastomlijnde kaders zijn en zij ervan op de hoogte zijn hoe moet worden omgegaan bij bijvoorbeeld concrete aanleidingen of vraagstukken waar privacy een rol speelt.
- Agendeer structureel de thema's informatiebeveiliging en bescherming van persoonsgegevens op de MT-agenda en leg de verbinding met andere thema's zodat beide abstracte thema's dichterbij komen voor medewerkers.
- Borg dat (breed) binnen de ambtelijke organisatie voldoende capaciteit, kennis en ervaring met betrekking tot informatiebeveiliging en bescherming van persoonsgegevens aanwezig is.
- Zorg voor tijdige opvolging van het huidige kleine, maar zeer ervaren team van CISO, FG en privacy officer, zodat de continuïteit wordt gewaarborgd.
- Voldoe aan de vereisten uit de AVG door:
    - het privacybeleid uit 2015 te actualiseren,
    - verwerkersovereenkomsten zodanig aan te passen dat ze voldoen aan de normen van de AVG.

Bijlage Ia.

Reactie college van B&W van Roermond op de rapportage van de RKC.

gemeente **Roermond**

uw nummer	RKC/2018/2
uw datum	10 april 2018
ons nummer	4786-2018
onze datum	15 mei 2018
verzonden	16 MEI 2018
inlichtingen bij	Dhr. W. Kaldenhoven
sector/afdeling	Secr/Secretaris
doorkiesnr.	0475 - 359 618
bijlage(n)	
betreffende	Bestuurlijk wederhoor inzake onderzoek Informatiebeveiliging en bescherming persoonsgegevens

Rekenkamercommissie van de gemeente Roermond
De heer mr. P.M.B. Schrijvers
Postbus 900
6040 AX ROERMOND

Geachte heer Schrijvers,

Op dinsdag 10 april 2018 heeft uw commissie het rapport 'Onderzoek Informatiebeveiliging en bescherming persoonsgegevens' voor bestuurlijk wederhoor aan ons college voorgelegd. Via deze brief ontvangt u onze reactie waarin wij ingaan op uw rapportage en dan met name op punten die aan ons college zijn gericht.

Wij zijn verheugd in het rapport te lezen dat u heeft geconstateerd dat de informatiebeveiliging en de bescherming van persoonsgegevens op orde is en ambtelijke door deskundige medewerkers goed is geborgd. U merkt op dat hoe meer men "boven in de organisatie" terechtkomt de gemeenteraad en in mindere mate het college op afstand staat van deze thema's.

Deels ligt dit in de aard en de bijbehorende vertrouwelijkheid van de onderzochte thema's zelf, maar uit uw aanbevelingen blijkt het toenemende belang van informatieveiligheid voor het goed functioneren van onze gemeente. Wij onderschrijven het belang hiervan. Om die reden zijn de thema's informatiebeveiliging en bescherming van persoonsgegevens met ingang van 2017 geplaatst op de agenda van het Auditcomité en wordt het comité op hoofdlijnen twee keer per jaar geïnformeerd over vertrouwelijke aangelegenheden, zonder daarbij bedrijfsvertrouwelijke informatie prijs te geven. Een aantal leden van de gemeenteraad, de voorzitter van de Rekenkamercommissie en de externe accountant zijn lid van dit comité.

In algemene zin kunnen wij ons vinden in de door u aan ons gedane aanbevelingen. De verdere uitwerking van deze aanbevelingen nemen wij op in ons uitvoeringsplan. Hierbij zullen wij ook stilstaan bij de vraag op welke wijze de raad beter in positie kan worden gebracht.

In de praktijk blijkt dat ook leden van de gemeenteraad betrokken willen zijn en (per omgaande) geïnformeerd willen worden indien zich calamiteiten voordoen (zoals een datalek, inbreuk in de informatieveiligheid en dergelijke. In dergelijke situaties is het gewenst is dat alle aandacht van de CISO en overige leden van het Computer Security Incident Response Team (CSIRT) en het daaruit voortvloeiend privacy team gaat naar het oplossen van het probleem en het indammen van de gevarensetting.

In dat geval zullen wij de raadsleden in eerste instantie uitsluitend informeren met een korte bevestiging van het beveiligingsincident en/of datalek. De focus van het CSIRT team moet liggen op het indammen van het gevaar en het onderzoek van de zaak. Zo snel als het CSIRT team zelf een objectief en compleet (of zo compleet mogelijk) beeld heeft van de situatie zullen zij via ons college de raad informeren.

In het rapport wordt in de algemene conclusie het punt aangeroerd dat de leeftijdsopbouw van de leden van het team Informatiebeveiliging en Privacy zorgen baart. Zowel de kwalitatieve opvolging als de continuïteit worden als punt genoemd. De focus van ons HRM programma ligt de komende jaren op, onder andere, het tijdig overdragen van kennis en het tijdig, op basis van een toekomstgericht profiel, werven van nieuwe medewerkers. De aanbeveling om te komen tot een verdere uitbreiding van dit team nemen we mee bij de integrale afweging in het proces van de begroting 2019.

Binnen afzienbare termijn zal het onderzoek Informatiebeveiliging en bescherming van persoonsgegevens worden voorzien van een uitvoeringsplan waarin wordt aangegeven hoe en op welke termijn uw aanbevelingen worden uitgewerkt.

Wij hopen u hiermee voldoende geïnformeerd te hebben.

Burgemeester en wethouders van Roermond,

De secretaris, De burgemeester,

mr. drs. J.J.Th.L. Geraedts M.J.D. Donders – de Leest

Bijlage Ib

Nawoord Rekenkamercommissie naar aanleiding van de reactie van het college van Burgemeester en Wethouders.

1 juni 2018

De Rekenkamercommissie heeft kennis genomen van de bestuurlijke reactie van het college burgemeester en wethouders van 15 mei 2018 op haar rapportage.

De positieve reactie van het college geeft geen aanleiding tot het maken van nadere opmerkingen.

De Rekenkamercommissie ziet uit naar de bespreking van het rapport in raad en commissie.

Bijlage II.

Onderzoeksrapport *“Informatiebeveiliging & bescherming van persoonsgegevens”.*

In opdracht van de RKC is het onderzoek uitgevoerd en het onderzoeksrapport opgesteld door: Berenschot.

Onderzoekers:
Il Shik Sloover
Randy Eichhorn
Rosa-May Postma
Anne van Heerwaarden

Berenschot

RKC Roermond

Informatiebeveiliging & bescherming van persoonsgegevens

Il Shik Sloover
Randy Eichhorn
Rosa-May Postma
Anne van Heerwaarden

23 maart 2018

Berenschot

RKC Roermond

Informatiebeveiliging & bescherming van persoonsgegevens

Inhoud **Pagina**

Berenschot

1. Inleiding

1.1 Aanleiding

De rekenkamercommissie (RKC) van de gemeente Roermond heeft in haar onderzoeksprogramma 2017/2018 het onderzoeksonderwerp ‘informatiebeveiliging en privacy’ opgenomen. De aanleiding van dit onderzoek naar informatiebeveiliging en bescherming van persoonsgegevens is door de RKC als volgt aangegeven:

Gemeenten hebben mede als gevolg van de decentralisaties in het sociale domein steeds meer persoonsgegevens in beheer. Ook wordt steeds meer informatie digitaal verwerkt en gedeeld met ketenpartners. Data en systemen worden in toenemende mate aan elkaar gekoppeld. In dat verband speelt het stelsel van Basisregistraties een belangrijke rol voor het uitvoeren van publiekrechtelijke taken door overheidsorganen (op centraal en decentraal niveau). Het is de bedoeling dat die organen verplicht gebruik maken van de gegevens in die basisregistraties.

De taken, bevoegdheden en verantwoordelijkheden van met name de colleges van B&W op het gebied van informatiebeheer en informatiebeveiliging, nemen als gevolg van deze ontwikkelingen sterk toe. Informatiebeveiliging is niet alleen van belang voor het goed functioneren van de overheidsorganisaties, maar zeker en vooral voor de borging van de informatieveiligheid van burgers. Informatieveiligheid wordt in toenemende mate een randvoorwaarde voor de inrichting en het functioneren van een professionele gemeentelijke organisatie. Bij informatieveiligheid gaat het om beschikbaarheid, vertrouwelijkheid en integriteit. Informatiebeveiliging betreft maatregelen om de informatieveiligheid te realiseren. Privacy gaat over de zorgvuldige omgang met persoonsgegevens en de bescherming van de persoonlijke levenssfeer van de inwoners.

Informatieveiligheid en privacy hebben slechts voor een deel te maken met techniek en ICT. Veilige omgang met informatie heeft voornamelijk te maken met de inrichting van de organisatie, de werkprocessen daarbinnen, beschermingsmaatregelen en de controle op alle drie. Maar ook met voortdurend bewustzijn bij bestuurders en medewerkers met betrekking tot privacy.

Om informatiebeveiliging te kunnen borgen in de gemeentelijke organisatie maakt de gemeente gebruik van een Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) die door de Informatiebeveiligingsdienst (IBD) is opgesteld. De IBD is een gezamenlijk initiatief van de VNG en VNG Realisatie. De IBD werkt voor alle gemeenten en richt zich vooral op bewustwording en (concrete) incidentondersteuning aangaande informatiebeveiliging. In dat verband werkt ook de VNG-visitatiecommissie Informatieveiligheid. Deze (tijdelijke) commissie adviseerde op basis van visitatiebezoeken gemeenten op bestuurlijk niveau over informatieveiligheid. De doelstellingen van deze commissie waren:

- aandacht voor informatieveiligheid bij gemeenten stimuleren en vasthouden
- vergroten/versterken van het handelingsperspectief van gemeenten op het terrein van informatieveiligheid
- toetsen of het systeem van verplichte zelfregulering werkt en hoe/waar dit verbeterd kan worden.

In het kader van dit onderzoek is het ook van belang stil te staan bij:

- de per 1 juli 2017 in werking getreden Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren en aan te laten sluiten bij de Planning & Control cyclus van de gemeenten.
- De huidige Wet bescherming persoonsgegevens (Wbp) is gebaseerd op een Richtlijn uit 1995[1] en wordt per 25 mei 2018 vervangen door een Europese verordening, de Algemene Verordening Gegevensbescherming (AVG)[2]. De AVG heeft directe werking[3] en gaat over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. De AVG is per 24 mei 2016 in werking getreden en de periode tot en met 24 mei 2018 is bedoeld als implementatieperiode in de EU-lidstaten. De AVG is van toepassing op alle 'verwerkingsverantwoordelijken'[4] (gemeenten vallen ook onder dit begrip) en regelt onder meer de transparantie van de verwerking[5] van persoonsgegevens, het verplicht aanstellen van een functionaris gegevensbescherming (FG) bij de overheid, het voldoen aan minimum inhoudelijke vereisten voor verwerkersovereenkomsten[6], de verplichting tot gegevensbescherming bij het ontwerpen van producten en diensten ('privacy by design') en het uitvoeren van een Privacy Impact Assessment (PIA). De Autoriteit Persoonsgegevens (AP) is de toezichthouder en kan forse boetes opleggen bij het niet nakomen van verplichtingen of overtreding van de AVG.

---

[1] Richtlijn 95/46/EG.

[2] Voor meer informatie over de AVG en de betekenis ervan voor gemeenten wordt verwezen naar het artikel 'Privacy en gemeenten: de Algemene Verordening Gegevensbescherming', in Gemeentestem 2017/132, Afl. 7460 - oktober 2017.

[3] Rechtstreekse werking wil zeggen dat ze particulieren en ondernemingen rechten geven waarop zij zich kunnen beroepen bij een nationale rechter.

[4] De AVG definieert verwerkingsverantwoordelijke als 'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.

[5] De AVG verstaat onder 'verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

[6] Onder de huidige Wbp wordt nog het begrip 'bewerkersovereenkomst' gebruikt voor de contractuele relatie tussen de gemeente en de derde partij (bijvoorbeeld een ICT-leverancier) die namens de gemeente persoonsgegevens bewerkt; vanaf 25 mei 2018 heet deze overeenkomst 'verwerkersovereenkomst'.

1.2 Doelstelling en vraagstelling

Doelstelling
Het doel van dit onderzoek is om na te gaan op welke wijze(n) de gemeente Roermond informatieveiligheid heeft georganiseerd en hoe in dat verband de werkprocessen daarop reeds zijn ingericht en hoe de bescherming van persoonsgegevens geborgd is.

Vraagstelling

1. Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?
2. Hoe geeft de gemeente Roermond vorm en inhoud aan het informatieveiligheidsbeleid?
3. Heeft de gemeente voldoende adequate maatregelen getroffen om de persoonsgegevens die zij in beheer heeft, te beschermen tegen de belangrijkste veiligheidsrisico's?

3a. Wat is de samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op samenwerking met derden en informatie-uitwisseling?[7]

4. Hoe is de communicatie / afstemming / sturing met betrekking tot het informatieveiligheidsbeleid tussen het college van B&W (college) en de ambtelijke organisatie geregeld?
5. Hoe is / wordt de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid vorm en inhoud gegeven?

De RKC heeft Berenschot opdracht gegeven om bovenstaande vragen te onderzoeken.

1.3 Leeswijzer

Dit rapport kent de volgende opbouw:

- Om inzicht te krijgen in de begrippen en afkortingen met betrekking tot de thema's informatiebeveiliging en bescherming van persoonsgegevens worden in paragraaf 1.4 een aantal afkortingen en begrippen nader toegelicht.
- In hoofdstuk 2 staat de verantwoording van het onderzoek centraal en wordt inzicht gegeven in de wijze waarop het onderzoek is uitgevoerd.
- In hoofdstuk 3 worden de bevindingen gepresenteerd met betrekking tot de vraag op welke wijze(n) de gemeente Roermond informatieveiligheid heeft georganiseerd en hoe in dat verband de werkprocessen daarop al zijn ingericht en hoe de bescherming van persoonsgegevens geborgd is.

[7] Vraag 3a is tijdens het onderzoek door de RKC toegevoegd.

- In hoofdstuk 4 worden aan de hand van de bevindingen uit hoofdstuk 3 de onderzoeksvragen beantwoord aan de hand van het door de RKC vastgestelde normenkader. Tevens treft u de door de RKC vastgestelde aanbevelingen aan.
- In de bijlagen zijn vervolgens opgenomen:
    - Respondentenlijst
    - Documentenlijst

1.4 Afkortingen- en begrippenlijst

Begrip	Afkorting	Toelichting
Adviesgroep Informatiebeveiliging en Privacy	Adviesgroep I&P	Adviesgroep Informatiebeveiliging en Privacy binnen de gemeente Roermond
Algemene Verordening Gegevensbescherming	AVG	De AVG geldt vanaf 25 mei 2018 voor de gehele Europese Unie en vervangt in Nederland de huidige Wet bescherming persoonsgegevens (Wbp). Gemeenten moeten ook voldoen aan de AVG.
Basisregistratie, stelsel van		Een basisregistratie is een door de overheid officieel aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit, die door alle overheidsinstellingen verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken.
Basisregistratie Adressen en Gebouwen	BAG	De BAG is de registratie waarin gemeentelijke basisgegevens over alle gebouwen en adressen in Nederland zijn verzameld.
Basisregistratie Grootschalige Topografie	BGT	De BGT wordt een uniform topografisch basisbestand met objecten in heel Nederland op een schaal van 1:500 tot 1:5.000. Het doel van de realisatie van de BGT is dat de hele overheid gebruik maakt van dezelfde basisset grootschalige topografie van Nederland. Topografie is de beschrijving van de fysieke werkelijkheid, dus de dingen die in het terrein fysiek aanwezig zijn.
Basisregistratie Personen	BRP	De BRP is de basisregistratie voor persoonsgegevens binnen het stelsel van basisregistraties. De Nederlandse overheid gebruikt de gegevens die in de BRP worden geregistreerd. Het gaat daarbij onder andere om naam, geboortedatum, geboorteplaats, verblijfplaats en familierelaties. Er zijn ook andere organisaties die de gegevens in de BRP gebruiken, zoals pensioenfondsen en onderzoeksinstellingen.
Baseline informatiebeveiliging	BIG	De BIG geeft op strategisch en tactische niveau een beschrijving van hoe een gemeente

Begrip	Afkorting	Toelichting
gemeenten		informatiebeveiliging kan inrichten. De BIG is afgeleid van de Baseline Informatiebeveiliging Rijksdienst (BIR) en voldoet aan de internationaal geaccepteerde beveiligingsstandaarden.
Buitengewoon opsporingsambtenaar	Boa	Een Boa is een beëdigd functionaris die bevoegd is tot de opsporing van bepaalde, meestal een beperkt aantal of een specifieke groep, strafbare feiten.
Chief Information Security Officer	CISO	De CISO is een functionaris binnen het vakgebied informatiebeveiliging die opereert op het grensvlak tussen business en techniek. Binnen de gemeente Roermond is deze rol belegd bij de adviseur informatiebeveiliging.
Datalek		Bij een datalek gaat het bijvoorbeeld om (onrechtmatige) toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Er wordt van een datalek gesproken als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking - dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.
Directieteam	DT	Het DT is het Directieteam van de gemeente Roermond en is samengesteld uit de gemeentesecretaris (voorzitter) en de directeuren.
Eenduidige Normatiek Single Information Audit	ENSIA	ENSIA is een nieuwe systematiek voor het auditen bij gemeenten met als doel dat de gemeente verantwoording aflegt aan ministeries inzake processen rondom de BRP, PNIK, BAG, BGT, Suwinet, DigiD en de implementatie van benodigde beveiligingsmaatregelen. Op basis van ENSIA zal er ook horizontale verantwoording over de status van informatieveiligheid plaatsvinden vanuit het college van B&W naar de gemeenteraad. De ingangsdatum voor ENSIA is 1 juli 2017.

Begrip	Afkorting	Toelichting
Functionaris voor de Gegevensbescherming	FG	Een interne toezichthouder op de verwerking van persoonsgegevens. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp) en vanaf 25 mei 2018 op basis van de Algemene verordening gegevensbescherming (AVG).
GAP-analyses		Een methodiek waarbij de huidige situatie en gewenste situatie worden vergeleken. Het verschil hiertussen is de “GAP”. De gap-analyse is een moment van terugkijken, reflecteren, evalueren en verbeteren.
ICT samenwerkingsverband Noord en Midden Limburg	ICT-NML	ICT NML is een samenwerkingsverband op basis van een gemeenschappelijke regeling tussen vier gemeenten (Venlo, Roermond, Weert en Nederweert) op het gebied van gezamenlijke ICT infrastructuur.
Management team	MT	Het management team van de gemeente Roermond
Meldplicht datalekken		Organisaties die een datalek hebben, moeten dit sinds 1 januari 2016 melden bij de Autoriteit Persoonsgegevens (AP) en soms ook aan de mensen van wie de gelekte gegevens zijn.
Planning en Control cyclus	P&C cyclus	De planning- en controlcyclus vindt zijn basis in de door de gemeenteraad vastgestelde Financiële verordening van de gemeente Roermond. Op grond van deze verordening biedt het college voor aanvang van het begrotingsjaar een overzicht aan, met daarin de data voor het vaststellen van de jaarstukken, kadernota, tussentijdse rapportage en de begroting met de meerjarenraming. Tevens geeft de verordening aan dat de criteria, waarop in deze stukken gerapporteerd zal worden in de desbetreffende stukken wordt toegelicht.
Plan-Do-Check-Act	PDCA	Cyclische benadering van continue kwaliteitsverbetering n.a.v. het model van William E. Deming met 4 onderdelen. De vier activiteiten in de kwaliteitscirkel van Deming zijn:

Begrip	Afkorting	Toelichting
		PLAN: Kijk naar huidige werkzaamheden en ontwerp een plan voor de verbetering van deze werkzaamheden. DO: Voer de geplande verbetering uit. CHECK: Meet het resultaat van de verbetering en vergelijk deze met de oorspronkelijke situatie en toets deze. ACT: Bijstellen aan de hand van de gevonden resultaten bij CHECK.
Privacy Impact Assessment	PIA	Methodiek om in een vroeg stadium op een gestructureerde en heldere manier inzichtelijk te krijgen als organisatie wat de grootste privacy risico's zijn.
Privacy Officer		De Privacy Officer is verantwoordelijk voor het vormgeven van het privacybeleid, het ondersteunen van de organisatie bij het in kaart brengen van de risico's rondom het gebruik van persoonsgegevens en het geven van advies omtrent het conform de Wbp en AVG verwerken van persoonsgegevens.
Stuurgroep I&P		Stuurgroep Informatiebeveiliging en Privacy binnen de gemeente Roermond
Suwinet		Op Suwinet zijn diverse overheidsorganisaties aangesloten zoals gemeenten, UWV en SVB. Via dit besloten netwerk kunnen gegevens van burgers en organisatíes veilig worden uitgewisseld. De gemeenten zijn betrokken bij deze ketendienstverlening, in de rol van leverancier en afnemer. De gemeentelijke taken zijn benoemd in de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi).
Vergunningen Informatie Systeem	VIS	Vergunningen Informatie Systeem gemeente Roermond
Vereniging voor Nederlandse Gemeenten	VNG	De VNG is de koepelorganisatie van alle gemeenten. De VNG behartigt de belangen van de gemeenten, voert gemeenschappelijke diensten voor gemeenten uit en biedt haar leden een platform.
Verklaring van	VVT	De VVT is onderdeel van de PDCA-cyclus

Begrip	Afkorting	Toelichting
toepasselijkheid		informatiebeveiliging van de gemeente Roermond en geeft inzicht in de BIG-beveiligingsmaatregelen (norm voor de gemeenten) of die wel/niet/deels zijn geïmplementeerd of niet van toepassing zijn.
Wet bescherming persoonsgegevens	Wbp	In de Wbp zijn de regels voor de omgang met persoonsgegevens in Nederland vastgelegd. Deze wet geldt nog tot 25 mei 2018 en daarna is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie.
Wet maatschappelijke ondersteuning	WMO	Gemeenten moeten er voor zorgen dat mensen zo lang mogelijk thuis kunnen blijven wonen. De gemeente geeft ondersteuning thuis via de Wet maatschappelijke ondersteuning (Wmo).

2. Onderzoeksverantwoording

2.1 Onderzoeksaanpak

De onderzoeksaanpak bestaat uit de volgende onderdelen:

- Startoverleg

Op 27 september 2017 is een startoverleg geweest met een afvaardiging van de RKC, de portefeuillehouder, een afvaardiging van de ambtelijke organisatie en onderzoekers. In dit overleg is door onderzoekers een presentatie gehouden over de aanpak van het onderzoek en heeft de RKC een toelichting gegeven op de vraagstelling en het concept normenkader.

- Normenkader

De RKC heeft het normenkader voor het onderzoek vastgesteld op 2 november 2017.

- Documentenonderzoek

Door onderzoekers zijn diverse documenten bestudeerd. In de bijlage is een documentenlijst opgenomen. Een aantal documenten is vanwege de vertrouwelijkheid ervan op locatie ingezien.

- Interviews, groepsinterviews en case studies ‘Totstandkoming informatiebeveiligingsbeleid’ en ‘Zorgteam Roermond en privacy’

De bevindingen uit de documentenstudie zijn met behulp van de interviews getoetst. Er zijn interviews gehouden met onder meer (een afvaardiging van) de gemeenteraad, het college van b en w, griffier, gemeentesecretaris, diverse afdelingshoofden en medewerkers en enkele externe partijen. Daarnaast zijn er twee case studies uitgevoerd. De case studie ‘totstandkoming van informatiebeveiligingsbeleid’ is gekozen als referentiecasus omdat in dit beleid alle aspecten van informatieveiligheid samenkomen. Het gaat hier enerzijds om het opstellen van beleid, het vernieuwen en verbeteren van beleid en de manier waarop alle stakeholders worden betrokken. De case studie met betrekking tot het Zorgteam gaat over de bescherming van persoonsgegevens / privacy, integraal werken en welke blokkades regelgeving tot gevolg kan hebben met betrekking tot de dienstverlening. Het Zorgteam is als casus gekozen omdat er sprake is van een nieuw stelsel voor alle ondersteuningsvragen van inwoners en in het sociaal domein veel ketenpartners samenwerken en onderling gegevens uitwisselen.

Van elk (groeps)interview en de twee case studies is een verslag opgesteld door onderzoekers dat is voorgelegd aan de respondenten voor goedkeuring. In de bijlage is een respondentenlijst opgenomen.

- Rapportage

Met de RKC is een concept rapportage besproken. Hierna is de concept rapportage door de RKC voor ambtelijke wederhoor aangeboden voor een toetsing van het feitenrelaas.

3. Beoordeling

3.1 Inleiding

In dit hoofdstuk komen de bevindingen uit ons onderzoek aan bod. Er wordt hierbij een vaste indeling aangehouden, waarbij vanaf paragraaf 3.3 eerst de bevindingen aan bod komen en gevolgd worden door een toetsing van de bevindingen aan de betreffende normen.

Ook worden de bevindingen uit de twee case studies nader beschreven en wordt antwoord gegeven op de vraag op welke wijze(n) de gemeente Roermond de totstandkoming van het informatiebeveiligingsbeleid heeft georganiseerd en hoe in dat verband de werkprocessen daarop reeds ingericht zijn, respectievelijk op welke wijze(n) de gemeente Roermond de bescherming van persoonsgegeven heeft geborgd en hoe in dat verband de werkprocessen daarop reeds ingericht zijn.

In de volgende paragraaf wordt eerst het normenkader weergegeven dat is gebruikt in het onderzoek. Het normenkader dient als beoordelingskader van dit onderzoek en de onderzoeksvragen kunnen hieraan getoetst worden.

3.2 Normenkader

Het door de RKC vastgestelde normenkader voor het onderzoek is als volgt:

Deelvragen	***Normen***
1. Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?	• ISO 27001/27002 en Tactische baseline informatiebeveiliging Gemeenten. • De algemeen geaccepteerde norm stelt dat er een risico-afweging moet plaatsvinden.[8] • Binnen de ambtelijke organisatie worden met voldoende frequentie risicoanalyses en/of dreigingsanalyses gemaakt. • In de risicoanalyses en/of dreigingsanalyses zijn de belangrijkste risico's geïdentificeerd. • De risicoanalyses en/of dreigingsanalyses geven inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens.

[8] Dit is terug te vinden in de BIG hoofdstukken 6 (6.2.1, 6.2.2), 8 (8.1), 9 (9.1.1) en 10(10.1.3, 10.1.4, 10.2.3), 12 (12.1.1, 12.6.1).

Deelvragen	*Normen*
2. Hoe geeft de gemeente Roermond vorm en inhoud aan het informatieveiligheidsbeleid?	• De gemeente voldoet aan de BIG normen: hoofdstuk 5 (5.1, 5.1.2) beschrijft welke documenten er dienen te zijn en hoe deze documenten gewijzigd, beoordeeld en aangepast worden. • De gemeente Roermond heeft een informatiebeveiligingsbeleid dat is vastgesteld door het college van B&W. • Dit beleid is gepubliceerd en bekend bij de organisatie en is beoordeeld op basis van inzicht in risico's. • Taken, bevoegdheden en verantwoordelijkheden zijn inzichtelijk (op basis van BIG norm 5.1). • De gemeente Roermond beoordeelt op regelmatige basis het beleid en geeft aan hoe wijzigingen tot stand zijn gekomen (op basis van BIG norm 5.1.2).
3. Heeft de gemeente voldoende adequate maatregelen getroffen om de persoonsgegevens die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's? **3a. Wat is de samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op samenwerking met derden en informatie-uitwisseling?**	De gemeente voldoet aan de tactische baseline informatiebeveiliging Gemeenten en aan ISO 27001/27002 in globale zin. Daarbij heeft de gemeente Roermond technische en organisatorische maatregelen getroffen die de risico's doen afnemen. Deze onderdelen worden beschreven in met name vier hoofdstukken van de BIG 8 (personele beveiliging), 10 (bedieningsprocessen), 12 (verwerving van systemen) en 15 (naleving). De normen zijn hieronder nader uitgewerkt. *Personele beveiliging* • De gemeente Roermond heeft op het vlak van personeelszaken maatregelen genomen om het personeel te ondersteunen om de juiste keuzes te maken met betrekking tot gebruik van persoonsgegevens.

Deelvragen	*Normen*
	• De gemeente Roermond bewerkstelligt dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. • Rollen en verantwoordelijkheden zijn duidelijk bij indiensttreding, functiewijziging en bij uitdiensttreding. *Beheer van communicatie- en bedieningsprocessen* • De gemeente Roermond waarborgt een correcte en veilige bediening van ICT-voorzieningen. Er zijn duidelijke processen met betrekking tot het werken met persoonsgegevens (functiescheiding). *Verwerving, ontwikkeling en onderhoud van informatiesystemen* • De gemeente Roermond bewerkstelligt dat beveiliging integraal deel uitmaakt van informatiesystemen. Er is grip op correcte verwerking in systemen en validatie van invoergegevens en van uitvoerberichten. Er is beleid voor cryptografische beheersmaatregelen en beleid met betrekking tot uitlekken van informatie. • De gemeente voldoet aan de beleidsregels meldplicht datalekken • De gemeente legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek

Deelvragen	*Normen*
	en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. *Naleving* • De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
4. Hoe is de communicatie / afstemming / sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie geregeld?	• Er is periodiek overleg met betrekking tot het thema informatieveiligheid en privacy. • Tijdens dit overleg is er aandacht voor strategische, tactische en operationele vraagstukken. • Er is duidelijkheid bij betrokkenen over de betrokkenheid van en afstemming tussen de ambtelijke organisatie en het college bij de totstandkoming van beleid op het gebied van informatieveiligheid
5. Hoe is/wordt de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid vorm en inhoud gegeven?	• Er zijn tussen gemeenteraad en college afspraken gemaakt over rollen, taken en verantwoordelijkheden (‘spelregels’) en betrokkenen houden zich aan deze afspraken. • De aard van de gestelde kaders (output, hoe gaan we het doen?), proces (voorwaarden waarbinnen we het gaan doen), outcome (effecten die het beleid dient te hebben) sluiten aan bij het vraagstuk informatieveiligheid en privacy. • Er zijn afspraken gemaakt en vastgelegd over de informatievoorziening van college aan de gemeenteraad gedurende het proces van kaderstelling (vorm en moment informatie). • De kaders zijn SMART / meetbaar

Deelvragen	*Normen*
	geformuleerd. • De gemeenteraad heeft een informatiebehoefte gearticuleerd om grip te houden op het thema informatieveiligheid en privacy. • Door het college wordt voldaan aan de actieve informatieplicht. • De controle en bijsturing van de gemeenteraad is gericht op het realiseren of heroverwegen van de doelstellingen van het informatieveiligheidsbeleid en de bescherming van persoonsgegevens. • Het thema informatieveiligheid en privacy wordt periodiek geagendeerd in de gemeenteraad dan wel commissie.

3.3 Zicht op de belangrijkste risico's van informatiebeveiliging en bescherming van persoonsgegevens

De eerste onderzoeksvraag is of de gemeente in brede zin een goed beeld heeft van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens.

3.3.1 Bevindingen

Vanaf 2005 staat het thema informatieveiligheid op de agenda van de informatiseringsafdeling van de gemeente Roermond. Vanaf dat moment is vanuit het ambtelijk apparaat, de chief information security officer (CISO), begonnen met het opzetten van informatiebeveiliging op basis van de Code voor Informatiebeveiliging. Vanaf 2014 is de baseline informatiebeveiliging gemeenten (BIG) en het werken met GAP-analyses[9] geïntroduceerd, uitmondend in het opstellen van het huidige informatiebeveiligingsbeleid. Privacy c.q. bescherming van persoonsgegevens was een integraal onderdeel van dit beleid, maar is sinds de decentralisaties in het sociaal domein in 2014/2015 nadrukkelijker een eigen onderwerp geworden.

[9] Het doel van de GAP-analyse is te controleren of en in welke mate de maatregelen uit de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten geïmplementeerd zijn bij de gemeente die het onderzoek uitvoert of laat uitvoeren. De GAP-analyse bevat alle maatregelen uit de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) met daarbij controlevragen. De GAP-analyse is een methode om een vergelijking te maken tussen een bestaande of huidige situatie en de gewenste situatie, de maatregelen uit de baseline.

Aandacht en bewustwording

In individuele- en groepsgesprekken wordt de hiervoor beschreven gestage aandacht met betrekking tot de thema's informatiebeveiliging en bescherming van persoonsgegevens bevestigd. Ook wordt bevestigd dat de bewustwording van informatiebeveiliging en bescherming van persoonsgegevens binnen de organisatie is meegegroeid, net als de daadwerkelijke realisatie van maatregelen op het gebied van informatiebeveiliging en goede omgang met persoonsgegeven. Het overwegend positieve beeld dat de Visitatiecommissie Informatieveiligheid[10] van de VNG over voorgaande aspecten heeft, wordt bevestigd in de gesprekken met ambtelijke gesprekspartners waaronder MT-leden.

Vanuit individuele- en groepsgesprekken komt het beeld naar voren dat er sprake is geweest van groter wordende aandacht en bewustwording voor informatiebeveiliging en bescherming van persoonsgegevens bij leidinggevenden en ambtenaren. Het opbouwen van expertise en vertrouwen in de betrokken ambtelijke experts (CISO, senior adviseur privacy[11] en de privacy officer) heeft tot op heden geleid tot een positieve kruisbestuiving waarbij informatieveiligheid en bescherming van persoonsgegevens op het netvlies staan van gesprekspartners. Het resultaat van deze voortdurende inzet en stappen is dat alle personen met wie onderzoekers hebben gesproken duidelijk weten wie de CISO, senior adviseur privacy en de privacy officer zijn en bij wie men dus moet aankloppen bij vragen over informatie, risico's en maatregelen met betrekking tot informatiebeveiliging en privacy.

Proces

Het proces van informatiebeveiliging binnen de Gemeente Roermond is een cyclisch en iteratief proces, zeker als het gaat om risicomanagement. Vanuit het informatiebeveiligingsbeleid is de afspraak dat "voor elk kritisch bedrijfsproces en informatiesysteem namens het lijnmanagement periodiek een risicoanalyse wordt uitgevoerd voor het kwantificeren van de afhankelijkheden, de bedreigingen, de eisen en de benodigde maatregelen voor informatiebeveiliging."[12] Het informatiebeveiligingsbeleid is opgesteld door de CISO aan de hand van evaluaties, risicoanalyses, nieuwe inzichten, wensen en behoeften vanuit de organisatie en is vooraf besproken in het periodiek overleg met de adviesgroep informatiebeveiliging & privacy en de stuurgroep informatiebeveiliging & privacy. In praktijk is de BIG gevolgd en is voor de belangrijke primaire processen een baseline toets uitgevoerd. Samen met proces eigenaren is bekeken welke risico's er zouden kunnen optreden en of er aanvullende onderzoeken/maatregelen noodzakelijk zijn ten opzichte van de baseline. Van juni 2015 tot en met oktober 2017 zijn elf baseline toetsen uitgevoerd

[10] Raadsinformatiebrief Gemeente Roermond – 7027/2016 – 26 april 2016.

[11] Opgemerkt wordt dat overal waar in dit rapport de 'senior adviseur privacy' wordt genoemd, gelezen dient te worden dat deze inmiddels per 1 januari 2018 benoemd is tot de wettelijk verplichte Functionaris Gegevensbescherming.

[12] Informatiebeveiligingsbeleid versie 5.1, pagina 24.

(bijvoorbeeld Basisregistratie personen (BRP), Wet maatschappelijke ondersteuning (WMO) en SuwiNet). Risicomanagement binnen de informatiebeveiliging sluit aan bij de door de gemeenteraad in november 2012 vastgestelde Nota Risicomanagement en Weerstandsvermogen; er worden risico's in beeld gebracht, geanalyseerd en beoordeeld en hiermee bij de besluitvorming rekening gehouden door het college.

Voor de processen waarbij persoonsgegevens een rol spelen, zijn op basis van een door de privacy officer en de FG uitgevoerde risicoanalyse door de privacy officer en de FG of anderen PIA's uitgevoerd op het gebied van schuldhulpverlening, jeugdzorg en BSN. PIA's voor de Participatiewet, WMO en HRM zijn ingepland. Een PIA op het VIS is tot nu toe (nog) niet in de planníng opgenomen. In 2017 is een baselinetoets op (onder andere) VIS uitgevoerd waaruit blijkt dat het uitvoeren van een aanvullende PIA van toegevoegde waarde is. Men zet deze PIA's als instrument in om te bepalen wat de impact is van veranderingen/vernieuwingen in het proces specifiek op het gebied van privacy. Ook zijn er (zeer) recent bewerkersovereenkomsten gesloten met derden in het kader van de verwerking van persoonsgegevens. Het uitvoeren van PIA's en het sluiten van bewerkersovereenkomsten is conform de Wbp en ook de AVG.

De rapportages van de baseline toetsen, uitgevoerde PIA's en ondertekende bewerkersovereenkomsten bevatten inzichten in de belangrijkste risico's per bijbehorend proces. Tevens is voor enkele processen (bijvoorbeeld inzake BRP) een aanvullende, diepgaande risicoanalyse gedaan. Daarnaast hebben de privacy officer en de FG op basis van een risicoanalyse PIA's uitgevoerd of laten uitvoeren op het gebied van schuldhulpverlening, jeugdzorg en BSN en zijn PIA's voor de Participatiewet, WMO en HRM ingepland. In het Jaarplan Informatiebeveiliging 2017, dat is vastgesteld door het college op 6 juni 2017, staat verder een vooruitblik van hetgeen in 2017 zal worden opgepakt op basis van de 'Verklaring van Toepasselijkheid' (VVT) zoals die op 25 januari 2017 door het Directie Team is vastgesteld. In het Jaarplan Informatiebeveiliging 2017 is tevens opgenomen op welke onderwerpen de focus specifiek wordt gelegd zodat stappen voorwaarts gemaakt kunnen worden bij het implementeren van de BIG en wordt rekening gehouden met het tijdens het implementeren van het Privacybeleid toevoegen van activiteiten vooruitlopend op de AVG. Deze geplande acties zijn het resultaat uit periodieke zelfevaluaties, risicoanalyses, besprekingen, audit- en voortgangsrapporten.[13] Voorbeelden van aandacht voor specifieke risico's zijn de leidraad[14] die is opgesteld met betrekking tot het ontwerpen van nieuwe (analoge) formulieren en de interne vragenlijst[15] inzake het verwerken van persoonsgegevens en het treffen van beveiligingsmaatregelen bij de opstart van aanbestedingen. Ook is er een vastgelegde

[13] Bron: Jaarplan informatiebeveiliging 2017.

[14] De leidraad bevat een toelichting met betrekking tot welke specifieke privacyaspecten van belang zijn en met welke rekening moet worden gehouden.

[15] In de vragenlijst is opgenomen op welke wijze correct kan worden omgegaan met persoonsgegevens en informatiebeveiliging bij de aanschaf van producten en/of diensten.

procedure met betrekking tot het beheer van beveiligingsincidenten en een procedure voor het melden van datalekken.

College
Uit bovenstaande volgt dat de risico's in brede zin inzichtelijk zijn bij de ambtelijke organisatie, maar binnen het college en de gemeenteraad is er een ander beeld. Informatiebeveiliging en bescherming van persoonsgegevens zijn thema's die binnen het college wel leven, maar op een vrij hoog abstractieniveau. De Wethouder voor financiën, personeel en organisatie, grondzaken en eigendommen heeft bij de coalitieonderhandelingen de portefeuille informatieveiligheid toebedeeld gekregen. De wethouder vond deze keuze ook logisch omdat informatieveiligheid bij bedrijfsvoering hoort. Het thema privacy valt ook onder het thema informatieveiligheid en is dus onderdeel van zijn portefeuille.

De wethouder is vanuit zijn portefeuille primair verantwoordelijk voor beide thema's en hij informeert bij incidenten of calamiteiten. In de stuurgroep informatiebeveiliging & privacy, voorgezeten door de portefeuillehouder, wordt regelmatig gesproken over informatieveiligheid en bescherming van persoonsgegevens en op deze manier houdt het college de vinger aan de pols. Het college geeft als uitgangspunt aan dat informatieveiligheid en bescherming van persoonsgegevens goed geregeld moet zijn en dat men vertrouwen heeft in de ambtelijke expertise. In het groepsgesprek met het college werd aangegeven dat het hacken van buitenaf door derden als grootste risico wordt gezien, gevolgd door inbreuk op persoonsgegevens van burgers. In het kader van de decentralisaties in het sociaal domein is privacy in het college wel een thema dat speelt, maar het gesprek over informatiebeveiliging en privacy gaat het college met elkaar aan als er iets dringends naar voren komt als een incident.

Gemeenteraad
In het groepsgesprek met een delegatie van raadsleden wordt aangegeven dat informatiebeveiliging en privacy als relatief nieuwe onderwerpen worden gezien en men is nog op zoek naar de juiste koers. De delegatie van raadsleden geeft aan op afstand van deze materie te staan en geeft aan dat zij onvoldoende inzicht heeft in de risico's. Met het aanpassen van de regeling Auditcomité[16] is het mogelijk geworden dat binnen het Auditcomité overleg wordt gevoerd met het college over informatieveiligheid in niet openbare vergaderingen. In het groepsgesprek met een afvaardiging van de gemeenteraad werd aangegeven dat hacken van buitenaf door derden veruit als grootste risico werd gezien, direct gevolgd door inbreuk op persoonsgegevens van burgers.

Gemeenschappelijke regeling ICT-NMNL
Door Roermond wordt samengewerkt in een gemeenschappelijke regeling ICT Noord- en Midden-Limburg (Bedrijfsvoeringsorganisatie ICT-NML) op het gebied van onder meer systeem-, werkplek- en databasebeheer. Bij brief van 20 december 2017 is vanuit het college van B&W van gemeente Roermond aan ICT-NML gevraagd, naar aanleiding van de raadscommissie Bestuur en Middelen van 27 november 2017, hoe de nieuwe organisatie omgaat met informatiebeveiliging en

[16] Zie Raadsvoorstel 2016-040-1.

cybercriminaliteit en hoe dat geborgd wordt. Uit deze brief blijkt dat met betrekking tot informatiebeveiliging en privacy voor ICT-NML dezelfde regels en normen gelden als voor de gemeenten (onder meer BIG, Wbp/AVG, interne en externe toetsing van beveiligingsmaatregelen op basis van de ENSIA audit systematiek). Volgens het Informatiebeveiligingsbeleid heeft ICT-NML een security functionaris aangesteld voor dagelijks beheer van technische informatiebeveiligingsaspecten. De security functionaris van ICT-NML rapporteert aan de CISO van de gemeente Roermond en informatiebeveiliging is onderdeel van de service management rapportage. Het bestuur van ICT-NML bestaat volgens de gemeenschappelijke regeling uit een collegelid van iedere deelnemende gemeente. Elk lid van het bestuur verstrekt op grond van bepalingen in de gemeenschappelijke regeling zijn eigen college alle inlichtingen die worden gevraagd en het lid kan door zijn eigen college ter verantwoording worden geroepen of worden ontslagen. Ook is in de gemeenschappelijke regeling geregeld dat het bestuur de gemeenteraden alle informatie verstrekt die door één of meer leden van die raden worden gevraagd. Op basis van hiervoor genoemde toepasselijke regels en normen en bovenstaande interventiemogelijkheden op basis van de gemeenschappelijke regeling kunnen het college en de gemeenteraad van de gemeente Roermond aldus zicht houden op mogelijke risico's op het gebied van informatiebeveiliging en privacy.

3.3.2 Beoordeling aan het normenkader

In onderstaande tabel zijn de bevindingen getoetst aan het normenkader en wordt per norm een toelichting gegeven.

Norm	***Beoordeling***
ISO 27001/27002 en Tactische baseline informatiebeveiliging Gemeenten: • **De algemeen geaccepteerde norm stelt dat er een risico-afweging moet plaatsvinden.**[17] • **Binnen de ambtelijke organisatie worden met voldoende frequentie risicoanalyses en/of dreigingsanalyses gemaakt.** • **In de risicoanalyses en/of dreigingsanalyses zijn de belangrijkste risico's geïdentificeerd.** • **De risicoanalyses en/of dreigingsanalyses geven inzicht in specifieke risico's met betrekking tot het**	De gemeente voldoet aan het normenkader: Het doen van risico analyses is opgenomen in het beleid (v5.0) en wordt toegepast in de praktijk. In de periode juni 2015 tot en met oktober 2017 zijn elf baseline toetsen uitgevoerd binnen de gemeente Roermond. Daarnaast is risicomanagement in een breder verband opgenomen in de nota 'Risicomanagement en Weerstandsvermogen'. Mede op basis van baselinetoetsen zijn specifieke aanvullende risicoanalyses en PIA's uitgevoerd en zijn specifieke aandachtsgebieden benoemd in het Jaarplan Informatiebeveiliging.

[17] Dit is terug te vinden in de BIG hoofdstukken 6 (6.2.1, 6.2.2), 8 (8.1), 9 (9.1.1) en 10(10.1.3, 10.1.4, 10.2.3), 12 (12.1.1, 12.6.1).

Norm	***Beoordeling***
beheer van (bijzondere) persoonsgegevens.	Naast de formele documentatie werd bovenstaande beeld bevestigd in gesprekken, met afdelingshoofden die aangaven recent bevraagd te zijn over een PIA en/of baseline toets.

3.4 Vorm en inhoud geven aan het informatieveiligheidsbeleid

De tweede onderzoeksvraag is hoe de gemeente Roermond vorm en inhoud geeft aan het informatieveiligheidsbeleid.

3.4.1 Bevindingen

Informatieveiligheid kent een historie sinds 2005 binnen de gemeente met het volgen van de Code voor Informatiebeveiliging. De vorm en inhoud zijn in de basis gelegd door de CISO en later ook mede door de senior adviseur privacy en de privacy officer.

Mede door de aanhoudende inzet van de hiervoor genoemde functionarissen weerklinkt in het gesprek met het college, het geluid ‘we vertrouwen erop dat het goed geregeld is’. Dat is volgens de onderzoekers op te vatten als een mooi compliment vanuit het bestuur. De keerzijde van de medaille is de afhankelijkheid van een beperkt aantal personen met een zeer specifiek kennisprofiel waardoor gemeentelijke organisatie kwetsbaar is. Dit laatste beeld wordt ook bevestigd door de gemeentesecretaris, CISO, senior adviseur privacy en de privacy officer. Op het gebied van privacy/bescherming van persoonsgegevens zijn al de nodige stappen gezet. De privacy officer is per juli 2017 benoemd en de senior adviseur privacy (sinds oktober 2015 in dienst) is per 1 januari 2018 benoemd als FG. De CISO wordt in zijn werkzaamheden weliswaar ondersteund door een netwerk van collega’s die vanuit hun eigen rol en verantwoordelijkheid hun bijdragen leveren (bijvoorbeeld in het kader van ENSIA), maar met betrekking tot informatiebeveiliging is het leunen op één persoon een kwetsbaarheid. Voor de CISO wordt er bekeken of er ook een samenwerking met Leudal mogelijk is, aldus de gemeentesecretaris.

Qua aansturing vallen zowel CISO als de senior adviseur privacy (en beoogd FG) direct onder de gemeentesecretaris en hierdoor is er weinig discussie over de aansturing volgens de gemeentesecretaris. Doordat de CISO en de senior adviseur privacy dicht bij elkaar zijn gepositioneerd vindt er met de gemeentesecretaris en onderling kruisbestuiving plaats. Er is daardoor een beter beeld van en meer verwevenheid tussen informatiebeveiliging en privacy. De gemeentesecretaris houdt de kaders in de gaten van het beleid, blijft op de hoogte en stuurt aan waar dat nodig is. De CISO en senior adviseur privacy adviseren de gemeentesecretaris (en waar gewenst het Directie team (DT) en hebben daarbij een onafhankelijke rol. Zij gaan volgens de gemeentesecretaris het gesprek aan met de ambtenaren, DT en Management team (MT) en college vanuit een vrije rol; dit beeld wordt ook bevestigd in de gesprekken met MT-leden en ambtelijke medewerkers. In hoofdstuk 2.4 van het informatiebeveiligingsbeleid is expliciet uiteengezet wat de

taken en rollen zijn van de diverse betrokkenen binnen de gemeente. Op basis van de (groeps)gesprekken is de bevinding van onderzoekers dat de invulling van taken en rollen in de praktijk overeen komt met het beleid. Zo heeft het college van B&W het beleid vastgesteld, ziet de gemeentesecretaris toe op de uitvoering van het beleid en de taken die hieruit voortvloeien met betrekking tot informatiebeveiliging zijn belegd bij de CISO.

Binnen de gemeente zijn vijf overlegstructuren aan te wijzen waarin zowel de 'werkvloer', management, portefeuillehouder als vertegenwoordigers van de gemeenteraad een rol vervullen. Opvallend is dat de CISO in elk overleg een rol heeft, wat volgens onderzoekers aantoont dat deze functie, zoals hierboven reeds in het algemeen beschreven, kwetsbaar is omdat deze rol door één persoon wordt ingevuld.

Sinds de wijziging van de regeling van het Auditcomité per 14 juli 2016 heeft het Auditcomité een taak om overleg te voeren met het college over informatieveiligheid. Het Auditcomité bestaat uit drie vertegenwoordigers van de gemeenteraad, een vertegenwoordiger van de RKC, de portefeuillehouder Financiën, de concerncontroller en het hoofd van de Afdeling Concernadvies. Het Auditcomité vergadert circa 3-4 keren per jaar en handelt in het overleg met het college naar bevind van zaken en bepaalt wanneer en op welke wijze het gewenst is de gehele gemeenteraad over bepaalde elementen van informatieveiligheid te informeren.

De Werkgroep informatiebeveiliging vergadert periodiek naar bevind van zaken en draagt zorg voor de implementatie van het informatiebeveiligingsbeleid. De werkgroep staat onder voorzitterschap van de CISO en bestaat verder uit applicatiebeheerders, teamleider ICT, teamleider Huisvesting & Services, teamleider Documentaire informatievoorziening en medewerkers met specialístische kennis van het thema van de werkgroep.

Daarnaast is er een adviesgroep informatiebeveiliging & privacy. Deze heeft binnen de gemeente een adviesfunctie richting de Stuurgroep of rechtstreeks aan de directie en richt zich met name op beleid en adviseert over tactisch/strategische informatiebeveiligingskwesties. De adviesgroep treedt volgens het privacybeleid tevens op als het 'privacyteam'. De adviesgroep overlegt circa eens in de maand en bestaat uit de concern controller, adviseur informatiemanagement, senior adviseur privacy, privacy officer (jurist) en de CISO die optreedt als voorzitter.

De stuurgroep informatieveiligheid bestaat uit de portefeuillehouder (is tevens voorzitter), gemeentesecretaris, hoofd Concernadvies, en CISO die optreedt als secretaris en senior privacy adviseur. Elk kwartaal wordt de voortgang besproken en vindt de bestuurlijke afstemming plaats van het informatiebeveiligingsbeleid.

Binnen de gemeente Roermond is er ten slotte ook een team control met een juridisch, financieel en concerncontroller dat wordt aangestuurd door de gemeentesecretaris. De CISO, de senior adviseur privacy en de privacy officer zijn hierbij aangesloten. Aan dit overleg neemt per 1 januari 2018 de privacy officer deel als vervanger van de FG gezien zijn verantwoordelijkheid in de uitvoering van beleid. De FG neemt alleen nog deel op (eigen) verzoek, onder andere afhankelijk van de agendapunten. Het overleg van het team control heeft meer een informatief karakter. Verdieping vindt plaats in afzonderlijke functionele overleggen tussen de secretaris en de leden van de

onderdelen control en informatiebeveiliging en privacy. Volgens de concerncontroller wordt dit overleg ingezet om met elkaar te spiegelen.

De risico's voor informatiebeveiliging worden in kaart gebracht via de BIG baselinetoetsen en waar nodig door een aanvullende diepgaande risicoanalyse. Een externe partij voert deze analyse uit blijkt uit de gesprekken. Op basis daarvan worden de risico's inzichtelijk gemaakt en actiepunten en prioritering geformuleerd ten behoeve van het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid is tot op heden meerdere malen aangepast (de huidige versie is versie 5.0, van 4 november 2016) en vastgesteld op 29 november 2016. Alle versies vanaf versie 3 van het beleid zijn voorbereid en opgesteld door de ambtelijke organisatie (CISO) en nadien vastgesteld door het college. De basis voor de laatste wijzigingen zijn wijzigingen in wet- en regelgeving of een organisatiewijziging en niet zozeer door verandering van maatregelen of controls zo blijkt uit het groepsgesprek met de CISO, senior adviseur privacy en privacy officer. Het informatiebeveiligingsbeleid is terug te vinden op het intranet (Intro) en daarmee gemakkelijk (passief) vindbaar. Om de risico's op het gebied van informatieveiligheid en bescherming van persoonsgegevens in beeld te krijgen wordt het informatiebeveiligingsbeleid ten minste eens in de drie jaren van een update voorzien of eerder indien noodzakelijk en wordt daarnaast gewerkt met een jaarprogramma. De stuurgroep bespreekt elk kwartaal de voortgang. In het vastgestelde Jaarplan Informatiebeveiliging (6 juni 2017) is de daadwerkelijke fasering, prioritering en planning opgenomen. Daarnaast is er ook een privacybeleid vastgesteld (30 juni 2015) waarin de beleidsuitgangspunten van het kader geschetst worden waarbinnen privacybeleid wordt gevoerd met onder meer een vaststelling van verantwoordelijkheden per functie. De onderzoekers constateren dat het privacybeleid nog geënt is op het huidige regime van de Wbp en nog niet is toegespitst op de AVG.

Uit het groepsgesprek met de CISO, senior adviseur privacy en privacy officer kwam naar voren dat, omdat de BIG een baseline is, er altijd ruimte is om verdere stappen te maken. Deze extra stappen moeten wel tot verbetering leiden in plaats van meer vragen of een gevoel van extra last. De balans tussen gebruiksvriendelijkheid en het voldoen aan regels vergt volgens hen continue aandacht. De gemeente Roermond kan zich nog verbeteren in het gedetailleerder beschrijven van processen en procedures en deze formeel vaststellen; in de praktijk wordt er al veel uitgevoerd maar dit is nog niet in de volle breedte vastgelegd, zo bleek uit het groepsgesprek met de CISO, senior adviseur privacy en privacy officer. Informatiebeveiliging en privacy zijn volgens de concerncontroller nog geen vast onderdeel van de reguliere P&C-cyclus, maar men wil er wel naar toe werken dat deze thema's een eigen Plan-Do-Check-Act-proces (PDCA-proces) krijgen.

Uit de (groeps)gesprekken kwam naar voren dat er binnen de gemeente een behoorlijke mate van bewustwording is op de thema's informatiebeveiliging en privacy. Ook wordt aangegeven dat bewustwording binnen de ambtelijke organisatie versterkt kan worden door medewerkers nog meer te betrekken. In het Jaarplan Informatiebeveiliging is hierover een aparte paragraaf opgenomen waarin de te nemen acties zijn uitgewerkt. Door onderzoekers is ook geconstateerd dat de lading van de thema's informatieveiligheid en privacy bij een aantal afdelingen geladen wordt vanuit het thema 'integriteit' en eigen professionaliteit bij het uitvoeren van de werkzaamheden van de medewerker.

Raadsstukken en collegestukken waar geheimhouding op rust liggen bij de griffie beveiligd ter inzage. De stukken kunnen op verzoek ingezien worden.

3.4.2 Beoordeling aan het normenkader

In onderstaande tabel zijn de bevindingen getoetst aan het normenkader en wordt per norm een toelichting gegeven.

Norm	*Beoordeling*
De gemeente voldoet aan de BIG normen: hoofdstuk 5 (5.1, 5.1.2) beschrijft welke documenten er dienen te zijn en hoe deze documenten gewijzigd, beoordeeld en aangepast worden. • **De gemeente Roermond heeft een informatiebeveiligingsbeleid dat is vastgesteld door het college van B&W.** • **Dit beleid is gepubliceerd en bekend bij de organisatie en is beoordeeld op basis van inzicht in risico's.** • **Taken, bevoegdheden en verantwoordelijkheden zijn inzichtelijk (op basis van BIG norm 5.1).** • **De gemeente Roermond beoordeelt op regelmatige basis het beleid en geeft aan hoe wijzigingen tot stand zijn gekomen (op basis van BIG norm 5.1.2).**	De gemeente voldoet aan het normenkader: • Er is een informatiebeveiligingsbeleid. Dit beleid is de afgelopen jaren regelmatig (her)beoordeeld, gewijzigd en opnieuw vastgesteld door de betrokken actoren in de organisatie (CISO, senior adviseur privacy en de privacy officer, DT en college). • Het informatieveiligheidsbeleid en het jaarplan zijn gebaseerd op de BIG. Met behulp van de GAP-analyse ontworpen door de IBD worden acties geprioriteerd. Het informatiebeveiligingsbeleid bevat inzicht in risico's en is ingericht op het mitigeren van deze risico's. • Het informatiebeveiligingsbeleid is meerdere malen aangepast, de huidige versie is 5.0, van 4 november 2016. • Alle versies van het informatiebeveiligingsbeleid vanaf versie 3 zijn geformuleerd vanuit de ambtelijke organisatie en vastgesteld door het college. • Het informatiebeveiligingsbeleid is terug te vinden op een eigen stek op het intranet (Intro) en daarmee gemakkelijk (passief) vindbaar. • De daadwerkelijke aanpak in termen van fasering, prioritering en planning is opgenomen in het Jaarplan Informatiebeveiliging dat door de CISO is opgesteld en nadien is vastgesteld door het college op 6 juni 2017. • Taken, bevoegdheden en verantwoordelijkheden zijn duidelijk beschreven in het

Norm	*Beoordeling*
	informatiebeveiligingsbeleid en privacybeleid. Alle betrokken kennen hun taken, bevoegdheden en verantwoordelijkheden met name in de kleine groep betrokkenen van CISO, senior adviseur privacy en de privacy officer. Daarnaast wordt dit in de organisatie herkend. • Tot op heden is circa elke twee jaar een evaluatie geweest en zijn onderdelen van het informatiebeveiligingsbeleid aangepast en is helder aangegeven waarom het beleid is aangepast. • Naast de formele documenten is op basis van de gesprekken een hoge mate van bewustwording geconstateerd met betrekking tot informatieveiligheid en privacy.

3.5 Maatregelen ter bescherming van persoonsgegevens

De derde onderzoeksvraag is of de gemeente voldoende adequate maatregelen heeft getroffen om de persoonsgegevens die zij in beheer heeft, te beschermen tegen de belangrijkste veiligheidsrisico's. Daarnaast is de vraag wat de samenhang is tussen informatiebeveiliging, privacy en maatschappelijke effecten op samenwerking met derden en informatie-uitwisseling.

3.5.1 Bevindingen

Het privacybeleid is door het college vastgesteld op 30 juni 2015. In dit beleidsstuk is beschreven op welke wijze de gemeente haar ambities wil realiseren, wat de reikwijdte is van het beleid, wie binnen de gemeente welke verantwoordelijkheid heeft en hoe een evenwichtig cyclisch systeem van checks & balances is geborgd in het Privacy Control Systeem. Het privacybeleid uit 2015 is echter nog niet geactualiseerd naar de AVG die per mei 2018 van toepassing wordt.
Er zijn inmiddels een aantal PIA's uitgevoerd (bijvoorbeeld bij schuldhulpverlening en in het kader van de decentralisaties in het sociaal domein). Vanuit privacy oogpunt liggen volgens de CISO, senior adviseur privacy en de privacy officer de grootste risico's bij de drie decentralisaties en staan er nog een aantal PIA's op de rol voor de WMO, de Participatiewet en HRM-processen. Verder zijn er een aantal (recente) bewerkersovereenkomsten gesloten met diverse partijen die in opdracht van de gemeente als 'bewerker' in de zin van de Wbp hebben te gelden. De onderzoekers constateren dat de gemeente met de inzet van al deze beschikbare formele middelen tot op heden voldoende adequate maatregelen heeft genomen om de persoonsgegevens te beschermen.

Het (nog) niet aanstellen van een FG is destijds een bewuste keuze geweest, aldus de gemeentesecretaris, omdat hierdoor de rolinvulling van de senior adviseur privacy vrijer kan zijn en minder accent ligt op de formele rol van toezichthouder. Per 1 januari 2018 is de senior adviseur privacy benoemd als FG conform de AVG.

Uit het groepsgesprek met de CISO, senior adviseur privacy en de privacy officer werd duidelijk dat in 2014 privacy als focuspunt is benoemd en een stappenplan opgesteld is. In het Jaarplan Informatiebeveiliging zijn de onderwerpen opgenomen die de aandacht vragen van de gemeente, zijn een prioritering en planning opgesteld en worden nieuwe trends en ontwikkelingen op het gebied van privacy beschreven die in de nabije toekomst aandacht zullen vragen van de gemeente. In het Jaarplan Informatiebeveiliging wordt rekening gehouden met de eigen normstelling op het gebied van personele beveiliging[18], bedieningsprocessen[19], de verwerving van systemen en naleving van wet- en regelgeving. Deze normstelling betreft het streven van de gemeente Roermond om per hoofdstuk van de BIG minimaal 80% gerealiseerd te hebben. Alleen bij ‘naleving van wet- en regelgeving’ is de eigen normstelling behaald en is geen aparte actie voorgeschreven in het Jaarplan Informatiebeveiliging. De onderzoekers constateren dat de eigen normstelling bij de ‘personele beveiliging’ en ‘verwerving van systemen’ op enkele procenten na is behaald en dat er specifieke aandacht voor deze onderdelen zijn in het Jaarplan Informatiebeveiliging. Bij de ‘bedieningsprocessen’ is het streven om ten minste 80% van de BIG maatregelen te hebben gerealiseerd op enkele procenten na niet behaald. Met betrekking tot de bedieningsprocessen wordt aangegeven dat een deel van de nog te implementeren maatregelen terug te vinden zijn in het Jaarplan informatiebeveiliging. Daarnaast zijn ook andere hieraan gerelateerde activiteiten in het Jaarplan informatiebeveiliging van belang.

Bij signalen van kleine datalekken of ongeregeldheden is volgens de gemeentesecretaris een procesafspraak gemaakt dat de primaire lijn van communicatie én advisering wordt gestart door de CISO en/of de senior adviseur privacy en de gemeentesecretaris. Bij meer impactvolle zaken wordt volgens de gemeentesecretaris ook de verantwoordelijke portefeuillehouder gelijktijdig geïnformeerd. De CISO en privacy officer bewaken dat zaken worden opgepakt. Afhankelijk van de omvang en de mate waarin bijvoorbeeld een datalek de gemeente, externe partijen en gevoelige gegevens betreft, worden de portefeuillehouder en de betreffende vakwethouder geïnformeerd. Er wordt volgens de gemeentesecretaris niet gewerkt met een checklist of afwegingskader waarmee een keuze wordt gemaakt of men overgaat tot het melden van een lek. De afweging om wel of niet te melden wordt door de gemeentesecretaris gemaakt door een combinatie van advies van de senior adviseur privacy en CISO, eigen inzicht en onderbuikgevoel. In geval van (vermeende) grote impact neemt de gemeentesecretaris een besluit na afstemming met betrokken bestuurder(s). De

[18] Bij personele beveiliging gaat het om het bewerkstelligen van bewust zijn van bedreigingen en gevaren voor informatiebeveiliging bij in dienst komen, uit dienst treden en wijziging van functies.

[19] Bij bedieningsprocessen betreft het normen met betrekking tot hoe om te gaan met de in gebruik zijnde systemen, zoals het beschrijven van start- en afsluitprocedures, backupmogelijkheden etc.

portefeuillehouder wordt standaard van alle besluiten in kennis gesteld. Het bovenstaande proces kan mogelijk onbedoeld tot gevolg hebben dat er niet voldoende transparantie is naar het college en/of de gemeenteraad over signalen en zij kunnen daardoor onvoldoende op de hoogte zijn, ook van de zaken die geen impact hebben gehad.

Door een aantal MT-leden wordt aangegeven dat privacy af en toe op de agenda staat van het MT, maar niet structureel. Door twee MT-leden wordt aangegeven dat privacy onderdeel is van de beoordelingsronde. Men geeft aan dat de medewerkers zelf actief nadenken en bewust handelen met betrekking tot welke informatie gedeeld mag worden zowel intern binnen de gemeenten als naar buiten toe en hoe om te gaan met bijvoorbeeld concurrentiegevoelige of privacygevoelige informatie binnen de bestaande werkprocessen. Bij concrete aanleidingen en vraagstukken waar privacy een rol speelt wordt bij de afdeling Plannen en Projecten het onderwerp ingebracht in het werkoverleg door de ambtelijke medewerkers. Uit de gesprekken met ambtelijke medewerkers blijkt niet dat er een vastomlijnd werkproces is beschreven hoe hiermee moet worden omgegaan. Uit de gesprekken met ambtelijke medewerkers blijkt wel dat vrijwel alle medewerkers een hoge mate van bewustzijn etaleren met betrekking tot privacyaspecten. Tegelijk wordt in de gesprekken met de afdeling Publiekszaken, de gemeentesecretaris en in het groepsgesprek met de CISO, privacy officer en FG aangegeven dat privacy (structurele) aandacht vergt binnen de gemeente. Kwetsbaarheden liggen met name in de samenwerking (gegevensuitwisseling) met externe partners bijvoorbeeld in het sociale domein / de drie decentralisaties, blijkt uit het gesprek met de gemeentesecretaris respectievelijk het groepsgesprek met de CISO, privacy officer en FG.

Privacy speelt vooral in de werkdossiers een belangrijke rol als het gaat om informatie die dagelijks gebruikt wordt. Er wordt bijvoorbeeld binnen de afdeling bouwtoezicht gewerkt met een kopie van een dossier dat is samengesteld op basis van interne afspraken. Als er een rode stempel op het dossier staat, betekent dit dat informatie over een bepaald perceel en/of persoon niet extern gedeeld mag worden omdat de betreffende burger dat heeft aangegeven. Men zorgt ervoor dat alle informatie perceelgericht en niet persoonsgericht is. Dit heeft te ermee te maken dat de objecten (bijvoorbeeld gebouwen) het onderwerp van toezicht zijn. In het geval van Wabo-vergunningen geldt dat de aanvrager zelf kan aangeven of zijn gegevens gedeeld mogen worden en deze keuze wordt vervolgens door de medewerkers gevolgd.

Bij de afdeling Publiekszaken is het beeld dat de bewustwording van voldoende niveau is, met name ingegeven door de gewenning aan het moeten voldoen aan richtlijnen zoals in het kader van de BRP bij het uitgeven van paspoorten. Aangegeven wordt dat men weet hoe belangrijk het is om de audits te halen als gemeente. Tegelijk wordt het als lastig ervaren dat informatieveiligheid en privacy op gespannen voet staat met dienstverlening en bedrijfsvoering. Uit het gesprek met de afdeling Publiekszaken blijkt dat actief wordt uitgezocht welke informatie wel of niet gedeeld mag worden, maar het beeld is dat medewerkers daarbij niet altijd naar het belang van de klant lijken te kijken. In de case studie van de totstandkoming van het informatiebeveiligingsbeleid is aangegeven dat op het moment dat bijvoorbeeld privacy wordt genoemd, dit er toe kan leiden dat men zich hierachter verschuilt, en dat het dan niet meer mogelijk is om bepaalde zaken uit te voeren vanwege privacy redenen.

3.5.2 Beoordeling aan het normenkader

In onderstaande tabel zijn de bevindingen getoetst aan het normenkader en wordt per norm een toelichting gegeven.

Norm	*Beoordeling*
• **De gemeente voldoet aan de tactische baseline informatiebeveiliging Gemeenten en aan ISO 27001/27002 in globale zin. Daarbij heeft de gemeente Roermond technische en organisatorische maatregelen getroffen die de risico's doen afnemen. Deze onderdelen worden beschreven in met name 4 hoofdstukken van de BIG 8 (personele beveiliging), 10 (bedieningsprocessen), 12 (verwerving van systemen) en 15 (naleving).** • **Wat is de samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op samenwerking met derden en informatie-uitwisseling?**	De gemeente voldoet grotendeels aan het normenkader: op de thema's 'personele beveiliging, 'bedieningsprocessen' en 'verwerving van systemen' voldoet de gemeente net niet aan haar eigen opgelegde normstelling. *Personele beveiliging* Er is beleid met betrekking tot in dienst komen, uit dienst treden en wijziging van functies. In de interne zelfaudit is benoemd dat de score slechts enkele procenten afligt van het gewenste niveau. In het jaarplan Informatiebeveiliging 2017 is specifieke aandacht voor dit onderdeel en is er in de breedte aandacht gevraagd voor omgang met privacy gevoelige informatie. *Beheer van communicatie- en bedieningsprocessen* Het beheer van bedieningsprocessen blijft met de score op het zelf assessment net iets achter op de gewenste score. In het Jaarplan informatiebeveiliging zijn een aantal te implementeren maatregelen hiervoor opgenomen. *Verwerving, ontwikkeling en onderhoud van informatiesystemen* Dit gaat met name over aanschaf en ontwikkeling van hardware, software en IT diensten (onderhoud, (documentatie en processen). Ook hier blijft de score net iets achter ten opzichte van de zelf gestelde norm. In het jaarplan van 2017 zijn diverse maatregelen opgenomen binnen dit kader. Met name om alle contracten te laten voldoen aan de Wbp/AVG en op basis van privacy by design/default bij inkoop en verwerving.

Norm	Beoordeling
	Naleving Op het gebied van het hoofdstuk naleving wordt de eigen norm behaald en ligt de focus met name op privacy. *Samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op de samenwerking met derden en informatie-uitwisseling* Op basis van de documentatie en gesprekken is een lijn zichtbaar dat medewerkers zeer bedacht zijn bij de informatie-uitwisseling, zowel intern als in de relatie met derden. Er is een hoge mate van bewustwording en bewustzijn op het gebied van informatiebeveiliging en privacy en dat het bij uitstek gaat om gevoelige informatie. In de werkprocessen wordt rekening hiermee gehouden door bijvoorbeeld met kopieën te werken waarin object gebonden in plaats van persoonsgebonden informatie is opgenomen. Bij de afdeling Publiekszaken is een effect beschreven dat er een spagaat wordt ervaren tussen wat mag en wat relevant is voor de klant en dat deze lijn in de praktijk lastig is te trekken en dat hierdoor de dienstverlening aan burgers kan worden geraakt.

3.6 De communicatie/afstemming/sturing tussen college en ambtelijke organisatie

De vierde onderzoeksvraag is hoe de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie geregeld is.

3.6.1 Bevindingen

In het informatiebeveiligingsplan zijn de rollen en taken op het gebied van strategische, tactische en operationele vraagstukken beschreven voor respectievelijk stuurgroep, adviesgroep en werkgroep informatiebeveiliging & privacy. Deze groepen hebben periodiek overleg en zijn bedoeld voor afstemming met het doel om te komen tot een integraal beveiligingsbeleid en de uitvoering ervan. De CISO heeft in al deze groepen een rol en is de daarmee de ’linking pin’ tussen de werkvloer (operationele processen) en de portefeuillehouder. Met de recente aanpassing van de regeling van

het Auditcomité heeft het Auditcomité vanuit een audit en control taak ook een taak om overleg te voeren met het college over informatieveiligheid.

Uit het groepsgesprek met het college bleek dat het college een grote mate van vertrouwen heeft in de ambtelijke organisatie en dat de ambtelijke organisatie informatiebeveiliging en privacy goed regelen. Met dit vertrouwen is niets mis, zij het wel dat het college verantwoordelijkheid heeft voor het opstellen en uitvoering van beleid. De onderzoekers vinden het in die zin opmerkelijk dat uit het groepsgesprek met het college naar voren komt dat een paar maanden geleden het informatiebeveiligingsbeleid door het college zonder inhoudelijke discussie is aangenomen terwijl de collegeleden ook aangeven dat deze materie vrij abstract is voor hen. Dit sluit echter wel aan bij het door het college zelf geschetste beeld dat collegeleden met betrekking tot informatiebeveiliging en privacy hoofdzakelijk het gesprek met elkaar aangaan als er iets dringends naar voren komt (incidenten, calamiteiten). De interne communicatie over incidenten of calamiteiten loopt in eerste instantie via de gemeentesecretaris en de portefeuillehouder. Als er sprake is van een datalek wordt dit het in het college besproken en bij ernstige incidenten worden het voltallige college en de gemeenteraad geïnformeerd aldus de portefeuillehouder.

Uit het groepsgesprek met betrekking tot de totstandkoming van het informatiebeveiligingsbeleid bleek dat wijzigingen in het informatiebeveiligingsbeleid verlopen via het traject adviesgroep informatiebeveiliging & privacy naar stuurgroep informatiebeveiliging & privacy naar directieteam. Ten slotte wordt het beleid in het college ingebracht ter besluitvorming. De portefeuillehouder heeft zitting in het Auditcomité en is voorzitter van de stuurgroep informatiebeveiliging & privacy. Uit het gesprek met het college blijkt niet dat het college een actieve rol inneemt. Volgens de portefeuillehouder is de aandacht van informatiebeveiliging en privacy in de gemeentelijke organisatie wel groeiend. De portefeuillehouder ervaart dit sterk in de stuurgroep die verantwoordelijk is voor de strategische vraagstukken. Het gevoel van urgentie is hoog, er gebeurt veel, en door de wijze van aanpak en inrichten voelt de portefeuillehouder zich ‘op zijn gemak’, maar aandacht voor informatiebeveiliging en privacy blijft wel vereist.

3.6.2 Beoordeling aan het normenkader

In onderstaande tabel zijn de bevindingen getoetst aan het normenkader en wordt per norm een toelichting gegeven.

Norm	***Beoordeling***
• **Er is periodiek overleg met betrekking tot het thema informatieveiligheid en privacy.** • **Tijdens dit overleg is er aandacht voor strategische, tactische en operationele vraagstukken.** • **Er is duidelijkheid bij betrokkenen over de betrokkenheid van en afstemming tussen de ambtelijke organisatie en het**	Er wordt deels voldaan aan het normenkader. Er is periodiek overleg binnen de werkgroep-, adviesgroep- en stuurgroep informatiebeveiliging & privacy. Over deze overleggen zijn de operationele, tactische en strategische vraagstukken belegt en helder beschreven in het informatiebeveiligingsbeleid. Het college neemt geen actieve rol in bij de

Norm	*Beoordeling*
college bij de totstandkoming van beleid op het gebied van informatieveiligheid	totstandkoming van het beleid. Markant punt is dat het college recentelijk het informatiebeveiligingsbeleid aangenomen heeft zonder inhoudelijke discussie.

3.7 Invulling van kaderstellende en controlerende rol van de gemeenteraad met betrekking tot informatieveiligheid en privacy

De vijfde onderzoeksvraag is hoe de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid en privacy vorm en inhoud is/wordt gegeven.

3.7.1 Bevindingen

Uit het groepsgesprek met een delegatie van de gemeenteraad komt vaar voren dat er binnen de gemeenteraad geen besluit is genomen over de gewenste wijze van informatievoorziening met betrekking tot informatiebeveiliging en privacy vanuit het college. De gemeenteraad heeft geen expliciete informatiepositie voor ogen; de raad weet niet welke informatie hij wil hebben en waarover de raad geïnformeerd moet worden. De gemeenteraad reageert naar eigen zeggen slechts vanuit incidenten richting het college in het kader van zijn controlerende taak; heeft het college het wel goed gedaan ten aanzien van het incident? En wat gaat het college ondernemen? Informatiebeveiliging en privacy zijn volgens de griffier geen politiek gevoelige onderwerpen en hebben daardoor minder prioriteit vanuit de gemeenteraad. De gemeenteraad geeft zelf aan dat het vrij technische materie betreft die een hoge dosis van expertise verlangt, hetgeen in de gemeenteraad maar mondjesmaat aanwezig is. De bewustwording binnen de gemeenteraad is naar eigen zeggen nog in een beginstadium en groeiende maar in beperkte mate bleek uit het groepsgesprek met de gemeenteraad. De gemeenteraad geeft aan dat het daardoor lastig is om kaders te stellen en dat alleen een controlerende rol kan worden ingevuld.

Het bovenstaande beeld van de rolinvulling van de gemeenteraad wordt bevestigd in de (groeps-) gesprekken met onder meer de ambtelijke medewerkers, gemeentesecretaris, griffier, portefeuillehouder en college. De griffier geeft aan dat over het algemeen de raadsleden erop vertrouwen dat het college adequate maatregelen heeft getroffen om de informatiebeveiliging en privacy goed te organiseren en dat de ambtenaren hun werk op dit gebied adequaat uitvoeren.

Het college geeft in het groepsgesprek aan dat informatiebeveiliging en privacy tot dusver nog geen issue of prioriteit is geweest binnen de gemeenteraad. De gemeenteraad heeft geen proactieve of initiërende rol en geen directe kaders gesteld hoe om te gaan met informatiebeveiliging en privacy. Indirect ervaart het college wel het kader dat de gemeenteraad ook graag ziet dat het goed geregeld is. Het college geeft aan dat er een raadsinformatiebrief naar de gemeenteraad is gestuurd en dat de gemeenteraad met ingang van 2017 in een afzonderlijke paragraaf in de jaarrekening op de hoogte wordt gehouden over de activiteiten met betrekking tot informatiebeveiliging en privacy. Op deze manier houdt het college de gemeenteraad in positie.

Daarnaast is gebleken dat er meerdere beelden zijn van de taak- en rolinvulling van het Auditcomité. Vanuit CISO, senior adviseur privacy en de privacy officer wordt aangegeven dat het Auditcomité het platform is voor het college om meer inhoud te delen op het gebied van onder andere informatiebeveiliging en privacy. Vanuit de controller wordt aangegeven dat het Auditcomité als doelstelling heeft om een afstemmingsorgaan te zijn naar de gemeenteraad en ziet het als een orgaan waarin men het voorwerk doet en dieper over de problematieken kan praten omdat de specialistische kennis bij de gemeenteraad ontbreekt. Het Auditcomité is als een soort filter of klankbord tussen college en gemeenteraad gezet volgens de voorzitter van het Auditcomité. De gemeentesecretaris geeft aan dat de gemeenteraad via het Auditcomité in alle vrijheid kan worden geïnformeerd en die setting biedt tevens de mogelijkheid om de nodige diepgang in gedachtewisselingen en informatieverstrekking te garanderen zonder dat het een potentieel politiek onderwerp wordt. Op deze manier is de informatievoorziening met de gemeenteraad volgens de gemeentesecretaris adequaat en in afstemming met de gemeenteraad ingeregeld.

Vanaf medio 2016 is er overleg mogelijk in het Auditcomité over informatieveiligheid. Dit thema is geagendeerd in juni en december 2017. In juni 2017 is een presentatie over ENSIA gegeven en over Privacy (Wbp en AVG). In december 2017 zijn informatiebeveiliging en privacy weer geagendeerd en dit overleg is in afstemming met de portefeuillehouder georganiseerd. De rol van het Auditcomité op het gebied van informatiebeveiliging en privacy is nog nieuw en nog niet uitgekristalliseerd. De onderzoekers constateren verder dat betrokkenen diverse beelden hebben van de rol- en taakinvulling van het Auditcomité en dat met instemming van de gemeenteraad zelf de kaderstellende rol van de gemeenteraad min of meer is belegd in het Auditcomité. Enerzijds vanwege het vertrouwelijke karakter van de onderwerpen en anderzijds vanwege de benodigde technische kennis om echt een klankbord te kunnen zijn. Vanuit de gemeenteraad wordt het Auditcomité nog niet aangesproken of aangestuurd om de onderwerpen informatiebeveiliging en privacy op de agenda te zetten aldus de voorzitter van het Auditcomité.

3.7.2 Beoordeling aan het normenkader

In onderstaande tabel zijn de bevindingen getoetst aan het normenkader en wordt per norm een toelichting gegeven.

Norm	***Beoordeling***
• **Er zijn tussen gemeenteraad en college afspraken gemaakt over rollen, taken en verantwoordelijkheden ('spelregels') en betrokkenen houden zich aan deze afspraken.** • **De aard van de gestelde kaders (output, hoe gaan we het doen?), proces (voorwaarden waarbinnen we het gaan doen), outcome (effecten die het beleid dient te hebben) sluiten aan bij het vraagstuk informatieveiligheid en**	Er wordt niet of nauwelijks aan het normenkader voldaan: Er zijn geen specifieke spelregels over hoe de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatiebeveiliging en privacy vorm en inhoud is/wordt gegeven. Er zijn ook geen specifieke afspraken over gestelde kaders, voorwaarden en output. Er zijn geen specifieke afspraken gemaakt over

Norm	*Beoordeling*
privacy. • **Er zijn afspraken gemaakt en vastgelegd over de informatievoorziening van college aan de gemeenteraad gedurende het proces van kaderstelling (vorm en moment informatie).** • **De kaders zijn SMART / meetbaar geformuleerd.** • **De gemeenteraad heeft een informatiebehoefte gearticuleerd om grip te houden op het thema informatieveiligheid en privacy.** • **Door het college wordt voldaan aan de actieve informatieplicht.** • **De controle en bijsturing van de gemeenteraad is gericht op het realiseren of heroverwegen van de doelstellingen van het informatieveiligheidsbeleid en de bescherming van persoonsgegevens.** • **Het thema informatieveiligheid en privacy wordt periodiek geagendeerd in de gemeenteraad dan wel commissie.**	de informatievoorziening van college aan de gemeenteraad met betrekking tot informatiebeveiliging en privacy. De gemeenteraad heeft geen specifieke informatiebehoefte aangegeven. In de regeling van het Auditcomité is weliswaar opgenomen dat het Auditcomité als taak heeft het voeren van overleg met het college van burgemeester en wethouders over informatieveiligheid, maar dit is echter niet specifiek ingestoken vanuit de gemeenteraad zelf. Er zijn geen kaders gesteld met betrekking tot informatiebeveiliging en privacy en derhalve zijn er geen kaders die SMART / meetbaar geformuleerd zijn. Door het college wordt op verzoek van de gemeenteraad voldaan aan de informatieplicht. Er zijn slechts op ad hoc basis vragen gesteld door de gemeenteraad en er is geen structurele aandacht voor het thema. De controle en bijsturing van de gemeenteraad is nihil. Er is daardoor geen sprake van het realiseren of heroverwegen van doelstellingen. Het thema informatiebeveiliging en privacy wordt nauwelijks geagendeerd in de gemeenteraad dan wel commissie. Aan het Auditcomité worden diverse rol- en taakinvullingen toegedicht. Deze diversiteit aan visies draagt nog niet adequaat bij aan de kaderstellende rol van de gemeenteraad. Vanuit de gemeenteraad of commissie wordt het Auditcomité nog niet aangesproken of aangestuurd om informatiebeveiliging en privacy op de agenda te zetten. Pas in juni 2017 is in het Auditcomité een presentatie over ENSIA en over Privacy (Wbp en AVG) gegeven en in december 2017 zijn informatiebeveiliging en privacy weer geagendeerd en dit overleg is in afstemming met

Norm	Beoordeling
	de portefeuillehouder georganiseerd. De rol van het Auditcomité op het gebied van informatiebeveiliging en privacy is nog nieuw en nog niet uitgekristalliseerd.

3.8 Case studie: Totstandkoming van het informatiebeveiligingsbeleid

De vraagstelling in de case studie is op welke wijze(n) de gemeente Roermond de totstandkoming van het informatiebeveiligingsbeleid heeft georganiseerd en hoe in dat verband de werkprocessen daarop al ingericht zijn.

3.8.1 Bevindingen

Zoals eerder aangegeven kent het informatiebeveiligingsbeleid van de gemeente Roermond een lange historie. Ambtelijk is er een sterke kern van personen bezig met de thema's informatiebeveiliging en privacy, onder directe aansturingslijn van de gemeentesecretaris. Het informatiebeveiligingsplan is een aantal keren bijgewerkt; dit actualiseren gebeurt ten minste eens in de drie jaren. Er is vanuit de gemeenteraad geen specifieke opdracht hiertoe gegeven en ook niet vanuit het college gaven de CISO, senior adviseur privacy en de privacy officer aan. Wijzigingen in het informatiebeveiligingsbeleid verlopen volgens de gesprekspartners via het traject adviesgroep informatiebeveiliging & privacy naar stuurgroep informatiebeveiliging & privacy naar directieteam en ten slotte wordt het beleid in het college ingebracht ter besluitvorming.

Het beleid is gevormd en aangepast aan de hand van diverse geplande externe gebeurtenissen, zoals het beschikbaar komen van de BIG, veranderingen in wetgeving (bijvoorbeeld de BRP, AVG) en de veranderingen in het sociaal domein. Deze externe triggers zorgden voor beperkte aanpassingen van het beleid die in klein comité van CISO, senior adviseur privacy en/of privacy officer voorbereid en gerealiseerd zijn. De initiatie van deze beleidsaanpassingen is zonder uitzondering opgepakt door de hiervoor genoemde adviseurs met inzet van hun expertise. Om de risico's op het gebied van informatiebeveiliging en privacy in beeld te krijgen wordt het Jaarplan informatiebeveiliging elk jaar van een update voorzien en wordt daarnaast gewerkt met een jaarprogramma. De stuurgroep informatiebeveiliging & privacy bespreekt elk kwartaal de voortgang.

Op beleidsniveau is recentelijk weinig communicatie over en weer met de ambtelijke organisatie geweest. In de voorbereiding van beleid, zoals bij het opstellen van jaarplannen, voorbereiden van audits en het uitvoeren van selfassessments is wel weer de samenwerking gezocht met de diverse afdelingen. Dit blijkt zowel uit diverse documenten zoals het Jaarplan Informatiebeveiliging 2017 dat is opgesteld door de stuurgroep informatiebeveiliging & privacy als uit gesprekken met betrokkenen zoals in het kader van het toegangsbeleid.

Het informatiebeveiligingsbeleid heeft een intern karakter. De gemeenteraad heeft in zeer beperkte mate haar kaderstellende en controlerende rol op het gebied van informatiebeveiliging en privacy opgepakt en toegepast met betrekking tot de totstandkoming van het informatiebeveiligingsbeleid.

3.8.2 Beantwoording van vraagstelling

De gemeente Roermond heeft over een lange periode een steeds verfijnder beleid ten aanzien van informatiebeveiliging en privacy opgesteld. Met een aantal belangrijke mijlpalen, zoals het werken conform de BIG en de decentralisaties in het sociaal domein is het bestaande beleid verder gepolijst. Vanuit de vraag hoe de gemeente de totstandkoming van het informatiebeveiligingsbeleid heeft georganiseerd, is te stellen dat de ontwikkeling van het informatiebeveiliging en privacy verder in de volwassenheidscyclus terecht gekomen is en dat daarmee de fase van opstarten en pionieren afgesloten is.

Tot op heden is het beleid tot stand gekomen door de focus, vastberadenheid en inzet van een klein team mensen (met name de CISO en senior adviseur privacy onder aansturing van de gemeentesecretaris). Zij hebben elk op hun eigen manier gezorgd voor het ontwikkelen, verbeteren en implementeren van het beleid.

De communicatie en afstemming in het kader van de totstandkoming van het informatiebeveiligingsbeleid is gegaan via de route werk-, advies-, stuurgroep informatiebeveiliging & privacy, dus vanuit de ambtelijke organisatie op een gestructureerde wijze naar uiteindelijk het college.

3.9 Case studie: Zorgteam Roermond en privacy

De vraagstelling in de case studie is op welke wijze(n) de gemeente Roermond de bescherming van persoonsgegeven / privacy heeft geborgd en hoe in dat verband de werkprocessen daarop reeds ingericht zijn.

3.9.1 Bevindingen

In het groepsgesprek is de nieuwe benaderingswijze van het zorgteam Roermond toegelicht. Ten opzichte van de oude situatie van aanvraag en beschikking, wordt er vanuit een sociale netwerkstrategie gekeken naar wat er voor de inwoner nodig is binnen alle leefdomeinen. De medewerkers van het zorgteam vormen de toegang naar maatwerk maar hebben daarbinnen de opdracht om het gehele sociale netwerk in kaart te brengen. De benadering is verschoven van ‘waar is recht op’ naar ‘wat is er nodig’.

Voorheen vroegen medewerkers van het Zorgteam toestemming om gegevens van cliënten te mogen verwerken aan de hand van een algemeen formulier. In de nieuwe werkwijze is nu vastgelegd dat bij constatering dat er op meer vlakken zaken spelen en er vanuit zorgverlening meer inzet nodig is, er specifieke toestemming gevraagd wordt aan de cliënt om met meer partijen en disciplines af te stemmen en gegevens te verwerken. De uitvraag voor informatie en de toestemmingsverklaringen zijn proportioneel en onafhankelijk volgens de gesprekspartners.

Daarnaast heeft de cliënt ook een gesprek met de medewerker van het Zorgteam waarin uitgelegd wordt waarvoor er getekend wordt en waarom ze over die informatie willen beschikken. Voor het zorgteam is aldus geprobeerd het proces voor medewerkers zo te faciliteren dat ze niet om bepaalde privacyaspecten heen kunnen. Privacy elementen zijn opgenomen in de normale werkprocessen en de standaarddocumenten zijn privacyproof gemaakt. Met betrekking tot privacy

gevoelige informatie wordt aangegeven dat men informatie op casus niveau niet deelt. Deze maatregel is ter borging van de privacy.

De gesprekspartners uit het zorgteam zijn zelf niet betrokken geweest bij de PIA's die zijn uitgevoerd maar zijn wel op de hoogte dat de PIA's worden uitgevoerd in het sociale domein. De wijkteams leefbaarheid en veiligheid hebben bijvoorbeeld zelf een PIA aangevraagd. Het zorgteam sluit ook aan bij wijkoverleggen. In die overleggen met onder andere politie, Boa's, woningcoöperaties en andere maatschappelijke partners heeft het wijkteam geconstateerd dat ze risico's lopen omtrent privacy. Er is daarom op eigen initiatief van het wijkteam een PIA aangevraagd.

Voor de inkoopcontracten van 2018 is gekeken naar wat de AVG voor hen betekent. In samenwerking en afstemming met de privacyfunctionarissen, eigen juristen en juristen van de omliggende gemeenten is dat verwerkt in de standaarddocumenten. Deze juristen en privacyfunctionarissen worden regelmatig betrokken bij de contracten, de afspraken over hoe persoonsgegevens gedeeld mogen worden en de eisen die ze aan aanbieders stellen. Zo moeten gedetacheerde krachten formulieren ondertekenen in het kader van privacy en geheimhouding.

Binnen de gemeente Roermond is er al geruime tijd een zekere mate van bewustwording rondom privacy. Dit bewustwordingsproces is gestimuleerd door de senior adviseur privacy, CISO en privacy officer. Er zijn workshops verzorgd voor het Zorgteam, uitvoerders, sociale wijkteams en beleidsmedewerkers halverwege 2015. In het algemeen ziet men dat medewerkers in het sociaal domein hun gedrag aanpassen zodat privacy geborgd wordt. Aan de andere kant is één van de grootste zorgen dat aandacht voor privacy ten koste gaat van werkbaarheid in de uitvoering aldus de gesprekspartners. Er is een tegenstrijdigheid tussen doelmatigheid in dienstverlening en privacy. Vanuit het oogpunt van privacy is integraal werken in het sociaal domein bijna onmogelijk, bijvoorbeeld bij jeugdhulp is het bijna onmogelijk om gegevens te delen, terwijl gemeenten de opdracht hebben vanuit het Rijk om alle zorg/hulp slim in te zetten. Een ander risico dat zich mogelijk kan voordoen is dat dienstverleners zich verschuilen achter de mogelijke schending van privacy, zonder voldoende te kijken of iets misschien wel of niet mogelijk is. Dit kan gevolgen hebben voor de dienstverlening aan de cliënt. Anderzijds zou het soms efficiënter zijn om gegevens wel uit te wisselen in het belang van de cliënt en de acute zorgvragen, maar men moet zich ervan bewust blijven dat de uitwisseling van gegevens een gevoelig onderwerp is.

3.9.2 Beantwoording van vraagstelling

Binnen het Zorgteam is met de start van de nieuwe aanpak gekozen voor een 'privacy by design' aanpak door het inzetten van privacyverhogende maatregelen en dataminimalisatie. Men heeft eerst een analyse gemaakt zodat een adequate doorvertaling heeft plaatsgehad van privacy in de werkprocessen. Bij de wijk- en zorgteams wordt de noodzaak tot het uitvoeren van een PIA onderkend, echter deze PIA's zijn (nog) niet uitgevoerd. Bij de inkoop van zorg is een werkproces ingericht zodanig dat er adequate ondersteuning is vanuit diverse juristen, maar ook op het gebied van privacy.

Er zijn workshops over privacy gehouden en de senior adviseur privacy, CISO en privacy officer hebben ook hun bijdrage geleverd aan de bewustwording binnen het Zorgteam. In het algemeen is

er binnen het sociaal domein een alertheid op privacyaspecten waarneembaar. De borging van privacy wordt herkend als noodzakelijk, maar men bemerkt in de praktijk dat privacy soms ook de dienstverlening in de weg staat en tegen het beleid van het Rijk indruist om integraal te kunnen werken binnen het gehele sociale domein.

4. Conclusies en aanbevelingen

4.1 Algemene conclusie

Uit het onderzoek komt het algemene beeld naar voren dat de gemeente Roermond de informatiebeveiliging en bescherming van persoonsgegevens goed heeft geregeld en dat vanuit de ambtelijke organisatie, met name vanuit de CISO, senior adviseur privacy/privacy officer en de gemeentesecretaris, de borging degelijk is. Wat verder opvalt, is dat de borging van deze twee thema's steeds zwakker wordt hoe meer men 'boven in de organisatie' terechtkomt, met name bij de gemeenteraad en het college. De gemeenteraad en het college staan op behoorlijke afstand van deze thema's, maar zij hebben wel vertrouwen in de ambtelijke organisatie dat zij goed omgaan met informatiebeveiliging en de bescherming van de persoonsgegevens en dat de ambtelijke organisatie het ook goed regelt.

De proactieve inzet van een klein aantal belangrijke functionarissen, te weten de CISO, senior adviseur privacy, privacy officer en de gemeentesecretaris, in afstemming met de portefeuillehouder, zorgt voor een inhoudelijke kruisbestuiving die op het gebied van informatiebeveiliging en bescherming van persoonsgegevens al jaren zijn vruchten afwerpt richting de gemeentelijke organisatie. Aan de huidige kleine bezetting van één CISO, senior adviseur privacy en privacy officer, de beperkte achtervang voor deze senior functionarissen en samenballing van deskundigheid binnen dit team kleven de risico's dat, mede vanwege de leeftijdsopbouw, zowel de opvolging als de continuïteit van dit team op korte termijn kwetsbaar zijn.

Aandacht binnen de ambtelijke organisatie van de gemeente Roermond voor de thema's informatiebeveiliging en bescherming van persoonsgegevens blijft echter wel vereist en dit geldt ook voor het college en de raad. Naast een hoge mate van bewustzijn binnen de ambtelijke organisatie worden de thema's informatiebeveiliging en bescherming van persoonsgegevens ook geladen vanuit andere thema's als integriteit en de eigen professionaliteit bij het uitvoeren van werkzaamheden.

Uit de eerste case studie met betrekking tot de totstandkoming van het informatiebeveiligingsbeleid volgt dat de ontwikkeling van het thema informatiebeveiliging verder in de volwassenheidscyclus terecht gekomen is en dat daarmee de fase van opstarten en pionieren afgesloten is. Het beleid is tot stand gekomen door de focus, vastberadenheid en inzet van een klein team mensen. De communicatie en afstemming in het kader van de totstandkoming van het informatiebeveiligingsbeleid is vanuit de ambtelijke organisatie op een gestructureerde wijze uitgevoerd.

Uit de tweede case studie inzake het Zorgteam is gebleken dat er een grote mate van aandacht en bewustzijn is met betrekking tot het thema privacy en het delen van gegevens. Eén van de zorgen is echter dat dit thema in het algemeen mogelijk ten koste kan gaan van doelmatigheid, de werkbaarheid voor medewerkers en dienstverlening aan burgers. Dit aandachtspunt geldt specifiek voor het gemeentelijke sociaal domein waarin integraal werken over de beleidsvelden heen de wens is, maar het als lastig wordt ervaren om gegevens te delen.

4.2 Beantwoording onderzoeksvragen

In onderstaande paragraaf worden de vijf onderzoeksvragen beantwoord.

1. Heeft de gemeente in brede zin een goed beeld van de belangrijkste risico's op het gebied van de informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens?

De gemeente Roermond heeft in brede zin een goed beeld van de risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van de persoonsgegevens.

De bewustwording van informatiebeveiliging en bescherming van persoonsgegevens is vanaf 2005 binnen de ambtelijke organisatie gegroeid. Bij het college en de raad leven de thema's informatiebeveiliging en bescherming van persoonsgegevens wel, maar staan op een vrij hoog abstractieniveau. Binnen het college is de portefeuillehouder gepositioneerd om het college te informeren over de thema's. De raad staat op afstand van de thema's en heeft onvoldoende inzicht in de risico's.

In het informatiebeveiligingsplan, Jaarplan Informatiebeveiliging en privacybeleid wordt duiding gegeven aan de risico's die gezien worden. In meer operationele zin is het uitvoeren van risicoanalyses opgenomen in het actuele beveiligingsbeleid en wordt dit toegepast in de praktijk, bijvoorbeeld door het uitvoeren van baseline toetsen en privacy impact analyses. In de periode juni 2015 t/m oktober 2017 zijn bijvoorbeeld 11 baseline toetsen uitgevoerd binnen de gemeente Roermond. Mede op basis van baselinetoetsen zijn specifieke aanvullende risicoanalyses en privacy impact analyses uitgevoerd en zijn specifieke aandachtsgebieden terugvertaald in het Jaarplan Informatiebeveiliging.

2. Hoe geeft de gemeente Roermond vorm en inhoud aan het informatieveiligheidsbeleid?

Het informatiebeveiligingsbeleid is vanaf 2005 regelmatig (her)beoordeeld, gewijzigd en opnieuw vastgesteld door de betrokken actoren in de organisatie (CISO, senior adviseur privacy, MT en college). De taken, bevoegdheden en verantwoordelijkheden zijn duidelijk beschreven in het beleid. De wijzigingen van het beleid zijn besproken in de werkgroep, projectgroep en uiteindelijk stuurgroep informatiebeveiliging & privacy. Het informatiebeveiligingsbeleid is voor iedereen terug te vinden op het gemeentelijke intranet.

Het informatieveiligheidsbeleid en het Jaarplan Informatiebeveiliging zijn gebaseerd op de baseline informatiebeveiliging gemeente (BIG). Met behulp van de GAP-analyse worden acties geprioriteerd. Het informatiebeveiligingsbeleid bevat inzicht in risico's en is ingericht op het mitigeren van deze risico's. Naast de formele documenten is op basis van de gesprekken een hoge mate van bewustwording geconstateerd met betrekking tot informatiebeveiliging en privacy.

3. Heeft de gemeente voldoende adequate maatregelen getroffen om de persoonsgegevens die zij in beheer heeft, te beschermen tegen de belangrijkste veiligheidsrisico's?

De gemeente heeft maatregelen getroffen om de persoonsgegevens die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's. Het betreft maatregelen op het gebied van personele beveiliging, bedieningsprocessen, verwerving van systemen en naleving van wet- en regelgeving. In het Jaarplan Informatiebeveiliging 2017 zijn diverse maatregelen opgenomen in de

gevallen dat de eigen norm met betrekking tot personele beveiliging en verwerving van systemen net niet zijn behaald. Het beheer van bedieningsprocessen blijft met de score op het zelf assessment net iets achter op de gewenste score. Opvallend is dat er geen directe punten voor verbetering zijn opgenomen in het Jaarplan Informatiebeveiliging 2017.

3a. Wat is de samenhang tussen informatiebeveiliging, privacy en maatschappelijke effecten op de samenwerking met derden en informatie-uitwisseling

Op basis van de documentatie en gesprekken is een lijn zichtbaar dat medewerkers zeer bedacht zijn bij de informatie-uitwisseling, zowel intern als in de relatie met derden. Er is een hoge mate van bewustwording en bewustzijn op het gebied van informatiebeveiliging en privacy en het besef dat het bij uitstek gaat om gevoelige informatie. In de werkprocessen wordt rekening hiermee gehouden door bijvoorbeeld met kopieën te werken waarin object gebonden in plaats van persoonsgebonden informatie is opgenomen. Bij de afdeling Publiekszaken is een effect beschreven dat er een spagaat wordt ervaren tussen wat mag en wat relevant is voor de klant en dat deze lijn in de praktijk lastig is te trekken en dat hierdoor de dienstverlening aan burgers kan worden geraakt.

4. Hoe is de communicatie/afstemming/sturing met betrekking tot het informatieveiligheidsbeleid tussen het college en de ambtelijke organisatie geregeld?

Er is periodiek overleg binnen de werkgroep-, adviesgroep- en stuurgroep informatiebeveiliging & privacy. In deze overleggen zijn de operationele, tactische en strategische vraagstukken belegd en helder beschreven in het informatiebeveiligingsbeleid. Het college neemt geen actieve rol in bij de totstandkoming van het beleid en heeft een grote mate van vertrouwen in de ambtelijke organisatie en dat zij het goed regelen. Een markant punt is dat het college recentelijk het informatiebeveiligingsbeleid aangenomen heeft zonder inhoudelijke discussie, terwijl het college ook aangeeft dat deze materie voor hen vrij abstract is. De interne communicatie over incidenten of calamiteiten loopt in eerste instantie via de gemeentesecretaris en de portefeuillehouder en bij ernstige incidenten worden het college en de raad geïnformeerd.

5. Hoe is de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de informatieveiligheid en privacy vorm en inhoud is/wordt gegeven?

Een raadsdelegatie die de onderzoekers gesproken heeft, geeft te kennen dat informatieveiligheid en privacy vrij technische materie betreft die een hoge dosis van expertise verlangt, hetgeen in de raad maar mondjesmaat aanwezig is. De bewustwording binnen de raad is naar eigen zeggen nog in een beginstadium en groeiende maar in beperkte mate. Vanuit de raadsdelegatie is aangegeven dat het daardoor lastig is kaders te stellen. Zonder gestelde kaders is het adequaat invulling geven aan de controlerende taak (toetsen aan de kaders) niet mogelijk.

Er zijn door de raad geen specifieke spelregels vastgelegd over hoe de kaderstellende en controlerende rol van de gemeenteraad met betrekking tot de thema's informatiebeveiliging en privacy vorm en inhoud is/wordt gegeven. De raad heeft geen specifieke informatiebehoefte aangegeven aan het college met betrekking tot informatiebeveiliging en privacy waardoor er geen kaders zijn die SMART / meetbaar geformuleerd zijn. Door het college wordt op verzoek van de raad voldaan aan de informatieplicht, zij het dat de raad ad hoc vragen heeft gesteld. De controle en

bijsturing van de raad is echter nihil en er is daardoor geen sprake van het realiseren of heroverwegen van doelstellingen. Het thema informatiebeveiliging en privacy wordt nauwelijks geagendeerd in de raad dan wel commissie.

In de regeling van het Auditcomité is sinds medio 2016 opgenomen dat het Auditcomité als taak heeft het voeren van overleg met het college van burgemeester en wethouders over informatieveiligheid, maar dit is echter niet specifiek ingestoken vanuit de raad zelf. Aan het Auditcomité worden diverse rol- en taakinvullingen toegedicht. Deze diversiteit aan visies draagt nog niet adequaat bij aan de kaderstellende rol van de raad. Vanuit de raad of commissie wordt het Auditcomité nog niet aangesproken of aangestuurd om informatiebeveiliging en privacy op de agenda te zetten. Pas in juni 2017 is in het Auditcomité een presentatie over ENSIA en over Privacy (Wbp en AVG) gegeven en in december 2017 zijn informatiebeveiliging en privacy weer geagendeerd en dit overleg is in afstemming met de portefeuillehouder georganiseerd. De rol van het Auditcomité op het gebied van informatiebeveiliging en privacy is nog nieuw en nog niet uitgekristalliseerd.

4.3 Aanbevelingen

De volgende aanbevelingen zijn vastgesteld door de RKC naar aanleiding van het onderzoek:

Gemeenteraad

- Maak als gemeenteraad zo snel mogelijk een start, mede gelet op inwerkingtreding van de AVG per 25 mei 2018, met het stellen van kaders met betrekking tot informatiebeveiliging en bescherming van persoonsgegevens zodat men als gemeenteraad in stelling komt om te controleren en (bij) te sturen, overleg hierover met het college waarbij er aandacht is voor het SMART formuleren van de kaders bijvoorbeeld met betrekking tot risico's en kwetsbaarheden, maatregelen en middelen die bijdragen aan de continuïteit van dienstverlening en een prioriteitenstelling.
- Bepaal als gemeenteraad welke informatievoorziening benodigd is, bijvoorbeeld door bij raadsvoorstellen de onderwerpen informatieveiligheid en bescherming van persoonsgegevens expliciet op te nemen in het format van raadsvoorstellen, en stem de spelregels over de informatievoorziening en verantwoording af met het college.
- Ga met het college halfjaarlijks de discussie aan over informatiebeveiliging en bescherming van persoonsgegevens zodat de gezamenlijke 'sense of urgency' gevoed blijft.
- Leg expliciet vast hoe de informatievoorziening jaarlijks vanuit het Auditcomité richting de gemeenteraad gebeurt.
- Maak meer gebruik van het Auditcomité door informatiebeveiliging en bescherming van persoonsgegevens te (laten) agenderen en evalueer tweejaarlijks de rolinvulling van het Auditcomité ten aanzien van deze twee thema's c.q. heroverweeg dit zo nodig.

College

- Wees als college aanjager van de thema's informatiebeveiliging en bescherming van persoonsgegevens door deze thema's aan de vakgebieden van medewerkers te verbinden waardoor er continu communicatie, aandacht en bewustwording is voor deze thema's.

Betrek medewerkers bijvoorbeeld door jaarlijkse presentaties of workshops over informatiebeveiliging en bescherming van persoonsgegevens.

- Ga halfjaarlijks de discussie aan met de raad over de thema's informatiebeveiliging en bescherming van persoonsgegevens, bijvoorbeeld over de prioriteitenstelling van te nemen maatregelen in het kader van de AVG.
- Leg nog meer en expliciet vast met betrekking tot de werkprocessen en procedures behorend bij informatiebeveiliging en privacy waardoor er voor medewerkers vastomlijnde kaders zijn en zij ervan op de hoogte zijn hoe moet worden omgegaan bij bijvoorbeeld concrete aanleidingen of vraagstukken waar privacy een rol speelt.
- Agendeer structureel de thema's informatiebeveiliging en bescherming van persoonsgegevens op de MT-agenda en leg de verbinding met andere thema's zodat beide abstracte thema's dichterbij komen voor medewerkers.
- Borg dat (breed) binnen de ambtelijke organisatie voldoende capaciteit, kennis en ervaring met betrekking tot informatiebeveiliging en bescherming van persoonsgegevens aanwezig is;
- Zorg voor tijdige opvolging van het huidige kleine, maar zeer ervaren team van CISO, FG en privacy officer, zodat de continuïteit wordt gewaarborgd.
- Voldoe aan de vereisten uit de AVG door:
    - het privacybeleid uit 2015 te actualiseren
    - verwerkersovereenkomsten zodanig aan te passen dat ze voldoen aan de normen van de AVG.

Berenschot

Bijlage: Respondentenlijst

Geïnterviewde	Functie
Han Geraedts	Gemeentesecretaris
Jos Vervuurt	Raadsgriffier
Frans Schreurs	Wethouder voor financiën, personeel en organisatie, grondzaken en eigendommen
Ernest Oele	Voorzitter Audit comité
Paul Ploum	Privacy officer
Huub Mulders	Sr. privacy officer / functionaris gegevensbescherming
Frans Laumen	Sr adviseur informatiebeveiliging / CISO
Pieta Tops, Roger Verbeek	Afdeling voorbereiding en realisatie
Wim Kaldenhoven	Concerncontroller
Marco Penders	Hoofd afdeling concernadvies
José Korteland, Sandra Amory	Afdelingshoofd plannen en projecten
Manuela Hendrix	Afdelingshoofd publiekszaken
Marcel Peusen, Sandra Slijpen, Nicole Verstegen	Case study Zorgteam
Ger Huijs, Guido Gootzen, Leanne Hodzelmans, Nico van Rijn	Case study totstandkoming informatieveiligheidsbeleid
College van burgemeester en wethouders	Voltallig college van burgemeester en wethouders
Hay Hutjens Leon Coenen Wim Kemp Wilbert Dekker Ger Julicher Wim Maassen	Afvaardiging van zes raadsleden namens gemeenteraad

Berenschot

Bijlage: Documentenlijst

Beleidsdocumenten

ICT beveiligingsbeleid Roermond	Vastgesteld door MT: 20 juni 2012 Vastgesteld door College van B&W: 23 augustus 2012 Datum: Juni 2012 Versie: 3.3 Status: Definitief
Informatie beveiligingsbeleid Roermond v4.8	Datum: 17 maart 2014 Versie: 4.8 Status: Definitief Vastgesteld door MT: 26 maart 2014 Vastgesteld door College van B&W: 8 april 2014 Addendum d.d. 25 november 2015 Vastgesteld door MT: 6 januari 2016 Vastgesteld door College van B&W: 19 januari 2016
Informatie beveiligingsbeleid Roermond v4.8 (incl. addendum)	Datum: 17maart 2014 Versie: 4.8 Status: Definitief Vastgesteld door MT 26 maart 2014 Vastgesteld door College van B&W: 8 april 2014
Informatie beveiligingsbeleid Roermond v5.0	Datum: 4 november 2016 Versie: 5.0 Status: Definitief Vastgesteld door MT: 17 november 2016 Vastgesteld door College van B&W: 29 november 2016
Privacybeleid gemeente Roermond	Datum 11 juni 2015 Vastgesteld door het college van B&W op 30 juni 2015

Financiële documenten

Begroting Gemeente Roermond 2017	Raadsvoorstel door College van B&W op 20 september 2016 Vastgesteld door de gemeenteraad op 10 november 2016
Begroting bijlagenboek Gemeente Roermond	Raadsvoorstel door College van B&W op 20 september 2016 Vastgesteld door de gemeenteraad op 10 november 2016
Kadernota 2017 - raad	Raadsvoorstel door College van B&W op 14 juni 2016

	Vastgesteld door gemeenteraad op 14 juli 2016
Kadernota 2018 integraal	Raadsvoorstel door College van B&W op 30 mei 2017 Vastgesteld door gemeenteraad op 13 juli 2017

Audit rapportages (vertrouwelijk)

Divers

Werkprocedures en checklists

Interne vragenlijst inzake persoonsgegevensverwerking aanbesteding	Versie 1 mei 2017
Procedure beheer beveiligingsincidenten en datalekken	Vastgesteld 13 december 2017 door het DT Vastgesteld 2 januari 2018 door het College van B&W
Procedure voor gebruik clouddiensten v2.0	Datum: 7 december 2016 Status: Definitief
Procedure voor gebruik clouddiensten v2-2	Vastgesteld 13 december 2017 door het DT Vastgesteld door het College van B&W 2 januari 2018
Ontwerpen van nieuwe analoge formulieren	

Bewerkersovereenkomsten (vertrouwelijk)

Diverse bewerkersovereenkomsten gesloten tussen de gemeente en bewerkers tussen juni 2016 tot en met december 2017.

Raadsdocumentatie

Raadsbesluit aanpassing regeling Auditcomité	Raadsvoorstel op 6 juni 2016 Vastgesteld tijdens gemeenteraad van 14 juli 2016
Raadsvoorstel aanpassing regeling Auditcomité	Raadsvoorstel op 6 juni 2016
Raadsinformatiebrief inzake privacybeleid	Datum: 23 juli 2015 Verzonden: 27 juli 2015

Visitatiecommissie Informatieveiligheid

Verslag visitatiecommissie Roermond	Visitatie op 3 februari 2016 Datum verslag: 23 februari 2016 Ter kennisgeving aangenomen door College van B&W op 26 april 2016

Berenschot

Raadsinformatiebrief inzake visitatiecommissie informatieveiligheid	Datum: 26 april 2019 Verzonden aan gemeenteraad 29 april 2016
Aanbiedingsbrief visitatiecommissie informatieveiligheid	

Risico-analyses (vertrouwelijk)

Model dataclassificatie en Baselinetoets

Overige documenten (vertrouwelijk)

ICT jaarplan

Privacyprotocollen

Privacy Impact Assessments

Zelf-evaluaties

Overzicht kwetsbaarheidsmeldingen vanuit IBD

Schermafdrukken selectie uit TOPdesk

Presentatie BIG en ENSIA ten behoeve van Auditcomité

Presentatie Privacy - Wbp en AVG ten behoeve van Auditcomité