Vereniging van
Nederlandse Gemeenten

Informatieveiligheid en intergemeentelijke samenwerkingsverbanden

TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Colofon

Een product van de VNG en de Taskforce BID

Teksten

AEF

Vormgeving

Chris Koning (VNG)

Coördinatie

Jasja van Ark (VNG)

Harro Spanninga (Taskforce BID)

maart 2015

Inhoudsopgave

1 Informatieveiligheid vereist aandacht

Bewustwording van en sturing op informatieveiligheid door bestuurders en (top)management wordt steeds belangrijker. Incidenten zoals DigiNotar en recente publicaties[1] over Suwinet[2] maken duidelijk dat betrouwbare en vertrouwelijke gegevensuitwisseling tussen overheid en burgers nog geen vanzelfsprekendheid is. Overheden moeten sturen op het inzichtelijk krijgen van informatiebeveiligingsrisico's, bijvoorbeeld als het gaat om de schending van de privacywetgeving door het misbruik van persoonsgegevens en het nemen van maatregelen.

Ook gemeenten staan voor de opgave om informatieveiligheid beter te borgen. Deze opgave wordt vergroot met de uitbreiding van het takenpakket van de gemeente, door bijvoorbeeld de decentralisaties en de komst van de Omgevingswet. Hierdoor zal de intensiteit van gegevensuitwisseling en daarmee het belang van informatieveiligheid verder toenemen. Onder meer de Inspectie SZW en het CBP zijn onderzoeken gestart naar de informatiebeveiliging van individuele gemeenten.

Onder meer anticiperend op bovenstaande ontwikkelingen hebben gemeenten in 2013 tijdens de Buitengewone Algemene Vergadering (BALV) de resolutie *Informatieveiligheid; een randvoorwaarde voor de professionele gemeente* ondertekend.[3] In deze resolutie hebben gemeenten zich gecommitteerd om zichzelf te toetsen aan de hand van een normenkader, de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG).[4] In de Baseline is opgenomen wat burgers en bedrijven, maar ook de ketenpartners, van gemeenten mogen verwachten ten aanzien van hun verantwoordelijkheid voor informatieveiligheid.

Een specifiek aspect bij informatieveiligheid is dat gemeenten niet al hun werk zelfstandig uitvoeren, maar vaak in gezamenlijkheid met andere gemeenten hun taken organiseren. Gemeenten werken samen in een groot aantal samenwerkingsverbanden. Meestal wordt daarbij gekozen voor samenwerking op basis van de Wet gemeenschappelijke regelingen (Wgr), maar er zijn ook diverse andere vormen zichtbaar (zie tabel 1 in de bijlage).

Leeswijzer

Deze notitie biedt gemeentesecretarissen, CISO's en het management van samenwerkingsverbanden een handvat hoe informatieveiligheid geborgd kan worden in intergemeentelijke samenwerkingsverbanden. Dit wordt ingekleurd op basis van casuïstiek over informatieveiligheid voor Intergemeentelijke Sociale Diensten (hierna: ISD), maar de lessen die we trekken zijn breder dan alleen voor de keten van werk en inkomen. Na een toelichting op het belang van informatieveiligheid staan we stil bij de verantwoordelijkheidsverdeling tussen gemeenten en samenwerkingsverbanden en hoe deze verantwoordelijkheden vertaald kunnen worden naar de praktijk. Ook beschrijven we risico's en/of problemen die gemeenten en ISD's tegenkomen. De notitie sluit af met een lijst van stuurvragen en de te nemen stappen die gemeenten en samenwerkingsverbanden kunnen helpen om hun informatieveiligheid (beter) te borgen.

1 *De Burger bediend in 2013,* Ministerie van Sociale Zaken en Werkgelegenheid, 2013.
2 Gemeenschappelijke Elektronische Voorzieningen Suwi (GEVS) biedt Suwinet-partijen de mogelijkheid (1) bij elkaar (persoons) gegevens te raadplegen en over te nemen in eigen administratie, genoemd inkijken; (2) elkaar, gegevens, documenten of andere informatie te verstrekken, genoemd meldingen versturen. (Regeling SUWI).
3 Gebaseerd op: *Informatieveiligheid, randvoorwaarde voor de professionele gemeente, VNG,* 2013 http://www.vng.nl/files/vng/brieven/2013/attachments/20131031_resolutie-informatieveiligheid.pdf
4 *Baseline Informatieveiligheid Nederlandse Gemeenten (BIG),* IBD, 2013, https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/

2 Gemeentelijke verantwoordelijkheid informatieveiligheid

In de resolutie *Informatieveiligheid; een randvoorwaarde voor de professionele gemeente* hebben de gemeenten ingestemd met aantal voorwaarden voor de bestuurlijke en organisatorische borging van informatieveiligheid:[5]

- **Borging:** informatieveiligheid is onderdeel van collegeambities 2014-2018 en wordt ondergebracht in de portefeuille van één van de leden van het college van B&W.
- **Informatiebeveiligingsbeleid**: gemeenten stellen informatieveiligheidsbeleid vast aan de hand van de Baseline Informatiebeveiliging Gemeenten.
- **Risicoanalyse**: het informatiebeveiligingsbeleid wordt vertaald naar een informatiebeveiligingsplan gebaseerd op eigenstandige risicoafwegingen. Gemeenten zijn zich daarbij bewust van de (continu veranderende) informatieveiligheidsrisico's die ze lopen en nemen hierop adequate maatregelen. In het informatiebeveiligingsplan worden thema's als continuïteit, ketens/(inter)gemeentelijke samenwerking) en incidentmanagement uitgewerkt.
- T**oetsing en verantwoording**: gemeente maken het thema van informatieveiligheid transparant voor burgers, bedrijven en (keten)partners. De informatie vormt de basis voor jaarlijkse collegiale beoordeling (peer reviews) en het college informeert de gemeenteraad over de resultaten. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.
- **Leercyclus**: informatieveiligheid wordt bestuurlijk en organisatorisch geborgd door aansluiting in de reeds bestaande planning- en controlcyclus. Het doel hiervan is dat gemeenten door middel van leren en ontwikkelen, een blijvend bewustzijn voor informatieveiligheid ontwikkelen.

5 Gebaseerd op: *Informatieveiligheid, randvoorwaarde voor de professionele gemeente, VNG,* 2013.

3 Informatieveiligheid en gemeentelijke samenwerking

Uit het voorgaande volgt dat een portefeuillehouder binnen het college van B&W verantwoordelijk is voor de (prioritering van) beveiliging van informatie binnen de bedrijfs(werk)processen.[6] Deze verantwoordelijkheid wijzigt niet op het moment dat de gemeente besluit om een bepaalde dienst of taak uit te besteden of samen met andere gemeenten (intergemeentelijk) uit te voeren. De gemeente blijft als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Zo blijft de gemeente bijvoorbeeld, indien zij verwerker is van persoonsgegevens, ook verantwoordelijk voor bewerkersafspraken met de bewerker van deze persoonsgegevens op basis van de Wet bescherming persoonsgegevens (Wbp).[7] Op het moment dat gegevens buiten de organisatie worden bewerkt, bijvoorbeeld bij een ISD dan moet met de ISD als bewerker ook afspraken gemaakt worden over deze persoonsgegevens en hoe verslaggeving hierover wordt gegeven conform de Wbp.

Voorbeelden - Verantwoordelijkheden informatieveiligheid bij intergemeentelijke samenwerking

Samenwerkingsverband de Drechtsteden[8]

Binnen het samenwerkingsverband de Drechtsteden zijn de individuele gemeenten (Dordrecht, Papendrecht, Sliedrecht, Zwijndrecht, Alblasserdam en Hendrik-Ido-Ambacht) verantwoordelijk voor het gebruik van informatie. De uitvoering van het informatiebeveiligingsbeleid hebben deze gemeenten gemandateerd naar het samenwerkingsverband (ISD). Een regionaal portefeuillehouder Informatievoorziening en Automatisering coördineert de werkprocessen op het gebied van ICT. De regionaal portefeuillehouder kan afspraken over 'harde' ICT afdwingen, maar formeel heeft hij niets te zeggen over de wijze waarop gemeenten met hun gegevens omgaan en dus ook niet over de beveiliging hiervan. De ICT-systemen die gegevens bevatten, zoals de GBA en BAG, zijn met verschillende veiligheidsregels en -procedures omlijnd, waar de gemeenten elk apart regelmatig op worden geaudit.

Samenwerking De Bevelanden

De vijf Bevelandse gemeenten Borsele, Goes, Noord-Beveland, Kapelle en Reimerswaal hebben een openbaar lichaam ingesteld gericht op de uitvoering van bedrijfsvoeringsaspecten.[9] Onderwerp van samenwerking zijn onder andere de ICT en informatievoorziening. Hier wordt uitvoering aan gegeven op basis van door de gemeente(raden) vastgestelde beleidsplannen. Met het oog op coördinatie is een afstemmingsoverleg informatievoorziening ingericht. In dit overleg komen onderwerpen aanbod zoals de aanschaf van softwarepakketten en al het andere op het gebied van ICT- en softwaregebied. Overigens blijven de gemeenten autonoom in hun besluitvorming: elke gemeente beslist uiteindelijk zelf.[10]

Voor Suwinet is specifiek in de wet opgenomen dat elke afnemer (dus ook de gemeenten) verantwoor-

6 Gebaseerd op: *Informatieveiligheid, randvoorwaarde voor de professionele gemeente, VNG,* 2013.
7 http://www.cbpweb.nl/downloads_brochures/bro_fg.pdf
8 *Informatieveiligheid binnen ICT-samenwerkingsverbanden.* Taskforce BID, 2013, http://www.taskforcebid.nl/inspiratie/special-informatieveiligheid/
9 Gebaseerd op: *Gemeenschappelijke Regeling Samenwerking De Bevelanden*, Gemeente Goes, 2013, http://decentrale.regelgeving.overheid.nl/cvdr/XHTMLoutput/Actueel/Goes/298601.html
10 Gebaseerd op *Informatiebeveiliging in beeld*, 2014, Informatiebeveiligingsdienst (IBD).

delijk is voor de beveiliging van het gebruik van Suwinet.[11] Dat betekent ook dat verantwoording van en transparantie over informatieveiligheid voor een gemeente van belang blijft. Afhankelijk van de keuze voor de inrichting van het samenwerkingsverband bestaan er al dan niet dwingende voorschriften over transparantie en verantwoording.

Overigens beperkt de scope van deze notitie zich niet tot 'nieuwe' samenwerkingsverbanden, het gaat ook over bestaande samenwerkingsverbanden. Voor de meest voorkomende vormen van intergemeentelijke sociale diensten is hieronder een toelichting opgenomen.[12] Op basis van deze toelichting wordt vervolgens een vertaalslag gemaakt naar wat vraagt dit van de portefeuillehouder informatieveiligheid.

Publiekrechtelijke samenwerkingsvorm(en)

Openbaar lichaam[13]

Gemeenten die deelnemen aan een openbaar lichaam kunnen taken en bevoegdheden delegeren aan het openbaar lichaam (artikel 10:4 Awb). Op deze manier is de gemeente niet (direct) betrokken bij de uitvoering. De sturingslijn tussen de gemeente en het openbaar lichaam loopt grotendeels via opdrachtformulering en financiering. Echter, instrumenten voor verantwoording zijn juridisch bepaald. De samenwerkingspartners beschikken over drie verantwoordingsinstrumenten:[14]

- het verschaffen van inlichtingen
- het afleggen van verantwoording
- het ontslaan/terugroepen van vertegenwoordigers.

De uitwerking van deze instrumenten hangt af van het gekozen samenwerkingsverband en van de soort regeling.[15]

Centrumgemeente

Een centrumgemeente is een voorbeeld van openbaar lichaam. De deelnemers komen overeen dat bevoegdheden van een bestuursorgaan van de ene gemeente worden uitgeoefend door een bestuursorgaan van de andere gemeente. Het ene gemeentebestuur mandateert dus bestuursbevoegdheden aan het andere. Desondanks gelden in dit geval niet alle van de voornoemde verantwoordingsinstrumenten. Een centrumgemeente heeft een inlichtingenplicht aan de deelnemende gemeenten. Een centrumgemeente kan echter niet ter verantwoording worden geroepen. Aan een centrumgemeente kunnen wel algemene of specifieke instructies worden gegeven. Hiermee wordt de verantwoording ook enigszins gedekt (10:6 Awb). Ook hebben de deelnemende gemeente geen bevoegdheden ten aanzien van het ontslaan/terugroepen van vertegenwoordigers. Wel kan het mandaat worden ingetrokken, wat eenzelfde effect heeft (10:8 Awb).

11 Voor het veiligheidsbeleid van het gebruik van Suwinet zijn de VNG, UWV en SVB gezamenlijk verantwoordelijk. Het beheer in bedrijfsmatige zin is belegd bij het UWV en het technisch beheer bij BKWI, als onderdeel van het UWV.

12 Voor een volledig overzicht van mogelijke samenwerkingsvormen voor gemeenten wordt verwezen naar *Vormen van samenwerken voor gemeenten*, Vereniging Nederlandse Gemeenten, 2014.

13 Gebaseerd op: *Samenwerking tussen gemeenten op basis van de Wgr*, Vereniging Nederlandse Gemeenten, 2008 en *Intergemeentelijke samenwerking toegepast*, Vereniging Nederlandse Gemeenten, 2013.

14 Gebaseerd op: Wet gemeenschappelijke regeling (Wgr) o.a. de artikelen 16, 17, 18 en 19.

15 Er zijn verschillende soorten regelingen zoals een raadsregeling en een collegeregeling, waarvoor andere regels gelden: zie *Intergemeentelijke samenwerking toegepast*, Vereniging Nederlandse Gemeenten, 2013

Privaatrechtelijke samenwerkingsvorm(en)

Stichting

Een keuze voor een privaatrechtelijke samenwerking is meestal gebaseerd op financiële en/of fiscale (efficiency) voordelen. Het gaat daarbij vaak om kortlopende projecten c.q. contracten. Het komt echter ook voor dat er sprake is van samenwerking met een meer structureel karakter. Een voorbeeld hiervan is de gezamenlijke inzameling van huisvuil door een particulier bedrijf. Iets wat het privaatrecht niet kent is het recht van de gemeenteraad of individuele raadsleden om inlichtingen te vragen aan de algemene vergadering van aandeelhouders, het bestuur of de raad van commissarissen. Ook over de verantwoording moeten in het contract met de private partij separate afspraken voor worden gemaakt.

Een stichting is een vorm van een privaatrechtelijke overeenkomst. Juridisch gezien kent de stichtingsvorm een minimum aan dwingende voorschriften. Wel kunnen door gemeente statutair gezien toezichtmogelijkheden geschapen worden. Bijvoorbeeld dat de gemeente alle bestuursleden benoemt en dat voor bepaalde besluiten goedkeuring nodig is. In het kader van transparantie kunnen afspraken gemaakt worden over hoe de stichting zich verantwoordt of kan een raad van toezicht worden ingesteld waarin vertegenwoordigers namens de gemeenten zitting nemen.

De samenwerking met ketenpartners en gemeenten is een aandachtspunt. Specifiek voor Suwinet geldt dat naast gemeenten ook organisaties als het UWV en de Sociale Verzekeringsbank gebruik maken van Suwinet. Van gemeenten mag niet worden verwacht dat zij de verantwoordelijkheid voor informatieveiligheid van ketenpartners overnemen. Vice versa kunnen gemeenten hun verantwoordelijkheid voor informatieveiligheid niet naar ketenpartners of bijvoorbeeld softwareleveranciers overhevelen. In geval van Suwinet hebben de Suwi-partijen gezamenlijk een wettelijke opdracht ten aanzien van het in stand houden en door ontwikkelen van Suwinet.

4 De taak van een portefeuillehouder informatieveiligheid

De voorgaande beschrijving laat zien dat dwingende verplichtingen over verantwoording per samenwerkingsvorm kunnen verschillen. Dit geldt dus ook voor informatieveiligheid. Aangezien informatiebeveiliging een lokale verantwoordelijkheid is, is het de taak van de (regionale) portefeuillehouder informatieveiligheid om na te gaan welke afspraken er per type samenwerkingsverband nodig zijn om informatiebeveiliging te borgen en op welke wijze hierover verantwoording wordt afgelegd. De *eisen* aan deze verantwoording en borging zijn uiteraard per samenwerkingsvorm hetzelfde. De afspraken uit resolutie *Informatieveiligheid; een randvoorwaarde voor de professionele gemeente,* waar de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) onderdeel van is, zijn immers voor elke gemeente (en samenwerkingsverband) hetzelfde.

Voorbeeld – De taak van een portefeuillehouder

Samenwerkingsverband de Drechtsteden[16]
De Regionaal portefeuillehouder Informatievoorziening en Automatisering de Drechtsteden houdt zich bezig met de coördinatie van de uitvoering op het gebied van informatieveiligheid. Op bestuurlijk niveau coördineert en regisseert hij de werkprocessen op het gebied van ICT tussen de gemeenten van het samenwerkingsverband. Hij stemt deze processen en de informatiehuishouding op elkaar af.

Toch kan op basis van voorgaande beschrijvingen een aantal extra aandachtspunten geformuleerd worden als het gaat om intergemeentelijke samenwerking en de borging van verantwoording over informatiebeveiliging. Deze aandachtspunten worden onderverdeeld in enerzijds juridische aandachtspunten (waar liggen de verantwoordelijkheden en bevoegdheden) en anderzijds de organisatorische aandachtspunten (wat is belangrijk voor een goede inrichting van het werkproces). Om deze aandachtspunten zo goed mogelijk toepasbaar te maken in de praktijk wordt deze belicht vanuit het perspectief van de gemeente en het perspectief van het samenwerkingsverband.

Juridische aandachtspunten
Op basis van voorgaande beschrijving van de soorten samenwerkingsvormen wordt duidelijk dat al dan niet dwingende verplichtingen per vorm verschillen. Wat vraagt dit juridisch gezien van een gemeente/of portefeuillehouder informatieveiligheid per vorm?

- Het **openbaar lichaam** is de meest gebruikte én de zwaarste vorm van samenwerking. Zoals hierboven is toegelicht biedt de Wgr drie type verantwoordingsinstrumenten; het verschaffen van inlichtingen, het afleggen van verantwoording en het ontslaan/terugroepen van vertegenwoordigers. Deze wettelijke borging van de verantwoordingsinstrumenten kennen de andere twee vormen van samenwerking (de centrumgemeente en de privaatrechtelijke overeenkomst) niet. In de totstandkoming van de juridische voorwaarden over verantwoording is daarom geen specifieke aandacht nodig, wel als het gaat om de sturing op de naleving ervan.
- Een centrumgemeente is een vorm van een openbaar lichaam waarbij specifieke instructies nodig zijn ten aanzien van de verantwoording rondom informatieveiligheid. Bij de samenwerkingsvorm **centrumgemeente** moet de gemeente afspraken maken over het afleggen van verantwoording

16 Gebaseerd op: *Informatiebeveiliging in beeld*, informatiebeveiligingsdienst, 2014

door de centrumgemeente aan de gemeenten voor wie de dienstverlening wordt uitgevoerd. Zoals hierboven is duidelijk gemaakt, kan een centrumgemeente immers niet ter verantwoording worden geroepen. Evenals voor de vorm van de privaatrechtelijke overeenkomst geldt dat bij de totstandkoming van het samenwerkingsverband algemene of specifieke instructies ten aanzien van de verantwoording (inlichtingen) over informatieveiligheid nodig zijn.

- Bij een **privaatrechtelijke overeenkomst**, bijvoorbeeld in het geval van een stichting moet een gemeente separate afspraken maken over hoe de stichting zich verantwoordt ten opzichte van de portefeuillehouder informatieveiligheid (= gemeente). Zoals immers uit de bovenstaande analyse blijkt, kent de stichtingsvorm een minimum aan dwingende voorschriften, bijvoorbeeld als het gaat om verantwoording aan de deelnemende gemeente. Wel kan de gemeente statutair gezien toezichtmogelijkheden creëren, bijvoorbeeld door een lid in het bestuur af te vaardigen. Kortom, er moeten afspraken gemaakt worden over waarop en hoe verantwoording door de stichting wordt afgelegd aan de gemeente.

Voorbeeld – Informatieveiligheid en de centrumgemeente

Gemeente Heerlen[17]

Gemeente Heerlen fungeert in de regio als centrumgemeente en is onderdeel van Parkstad IT, een ICT-samenwerkingsvorm gebaseerd op de Wgr. De gemeente Heerlen faciliteert als centrumgemeente voor omringende gemeenten de ICT-infrastructuur. In dienstverleningsovereenkomsten tussen de centrumgemeente en omringende gemeenten zijn afspraken gemaakt over het dienstverlenings- en beveiligingsniveau.

Een dienstverleningsovereenkomst bevat in het algemeen afspraken waarmee de relatie tussen een opdrachtnemer en een opdrachtgever wordt geregeld. Deze afspraken hebben bijvoorbeeld betrekking de taak- en opdrachtomschrijving, de kwaliteitsaspecten (in het geval van informatie het normenkader van de BIG), financiële kaders voor de uitvoering van de taak, de duur van de overeenkomst en eventuele voorwaarden ten aanzien van de uitvoering.

Organisatorische aandachtspunten (perspectief gemeenten)

Naast bovenstaande specifieke juridische aandachtspunten is er een aantal generieke onderwerpen die – ongeachte de samenwerkingsvorm van centrumgemeente, openbaar lichaam of privaatrechtelijke overeenkomst, van belang zijn om als portefeuillehouder informatieveiligheid op te sturen.

- De BIG schrijft voor dat gemeenten informatieveiligheidsbeleid opstellen voor de coalitietermijn. Daarnaast wordt jaarlijks een informatieveiligheidsplan opgesteld waarin onder andere naast een expliciete risicoafweging van betrouwbaarheidseisen, keuzen voor en implementatie van maatregelen die voortvloeien uit de betrouwbaarheidseisen zijn opgenomen. Als gemeenten samenwerken is het de opgave om dit beleid en deze plannen op elkaar af te stemmen. Dit kan gerealiseerd worden door:
  - Een gemeenschappelijk normenkader te vast te stellen op basis van het landelijke normenkader de BIG, en daarin zoveel mogelijk gelijke keuzes te maken.
  - De planning- en controlcylus van de gemeente en het samenwerkingsverband op elkaar af te stemmen.
- Dit maakt het voor gemeenten en het samenwerkingsverband overzichtelijk om de eigen beleids- en planvorming overzichtelijk en efficiënt te houden
- Naast de verantwoordelijkheid van de bestuurlijk portefeuillehouder Informatieveiligheid ligt het in rede om de verantwoordelijkheid voor de uitvoering van het informatieveiligheidsbeleid te

17 Gebaseerd op: *Informatiebeveiliging in beeld*, informatiebeveiligingsdienst, 2014

beleggen bij de gemeentesecretaris in kader van zijn rol als hoofd van de gemeentelijke organisatie. Specifiek daar waar het gaat om het afstemmen coördineren van de afstemming over het beleidskader en de planning- en controlcyclus.

- Tot slot, is het van belang dat een gemeente informatieveiligheid borgt in nieuw te vormen en bestaande samenwerkingsverbanden. Voor deze laatste categorie is nodig dat bekeken wordt hoe de borging van en verantwoording over informatieveiligheid is geborgd. Dat vraagt van gemeenten dat zij:
  - zicht hebben op bestaande afspraken die zijn gemaakt in samenwerking en/of uitbesteding van taken
  - in hun Informatiebeveiligingsbeleid expliciet aandacht besteden aan de ketens/samenwerkingsverbanden waarin zij opereren en toelichten welke afspraken zijn gemaakt ten aanzien van de borging van en verantwoording over informatieveiligheid.

Organisatorische aandachtspunten (perspectief samenwerkingsverbanden)

Als gezegd: gemeenten blijven ook bij samenwerking verantwoordelijk voor de veiligheid van 'hun' informatie. Voor het samenwerkingsverband kan dit echter een lastig werkbare situatie opleveren, met name wanneer verwacht wordt dat het verband zich voegt naar het beleid van elke individuele opdrachtgevende gemeente. Dit kan deels worden voorkomen door de samenwerkende gemeenten te vragen op basis van gemeenschappelijke normenkader van BIG zich te beperken tot algemeen beveiligingsbeleid en bijhorende planvorming.

Het is dan aan het samenwerkingsverband, bijvoorbeeld de ISD om hier een Suwi-specifieke aanvulling op te doen, dit voorkomt dubbelwerk en inefficiëntie. Deze aanvulling vanuit een ISD kan het beleid en de uitvoering betreffen, indien het vormen van Suwi-specifieke beleid niet alleen belegd is bij de gemeente. Om dit proces tussen gemeenten goed te laten verlopen, is het minimaal raadzaam dat samenwerkingsverbanden:

- zich conformeren aan de BIG
- bij elke (nieuwe) taak expliciet aandacht geven aan de informatieveiligheidsaspecten
- via interne en externe audits en reguliere verantwoording aan deelnemende gemeenten inzicht geven in de manier waarop informatieveiligheid in de eigen organisatie wordt geborgd
- daarbij specifiek aandacht hebben voor de manier waarop de informatiebeveiliging binnen de eigen organisatie aansluit op het beveiligingsbeleid van de opdrachtgevende gemeenten.

Voorbeeld – Uitvoering audits intergemeentelijke samenwerking

Samenwerkingsverband de Service Centrum Drechtsteden[18]

Ook voor de uitvoering van audits is het van belang om afspraken te maken met het oog op het realiseren van bijvoorbeeld efficiencyvoordelen. Binnen het samenwerkingsverband van de Drechtsteden wordt eerst een heldere scope opgesteld, wat complex is omdat dit met alle aanwezige partijen in de keten moet gebeuren. Nadat de scope helder is, is een kader nodig over wat er vooraf in kaart gebracht die te worden en wat centraal en decentraal gebeurt. Juist een centrale functie kan namelijk mogelijkheden bieden voor efficiency. Vervolgens voert het samenwerkingsverband integraal security testen en auditwerkzaamheden uit. De zes gemeenten zelf zijn geen partij tijdens de uitvoering van de testen en het audittraject. Alle ICT draait namelijk bij Service Centrum Drechtsteden (SCD) met dus als voordeel dat er maar één in plaats van zes testen hoeven te worden uitgevoerd.

18 Interviews van de IBD, IBD, 2014, http://www.taskforcebid.nl/overheidslagen/gemeenten/interviews-van-de-ibd/

6 Checklists

De VNG heeft een operationeel stappenplan opgesteld, aan de hand waarvan een gemeente kan komen naar een veiliger Suwinet.[19] Bij het (her)inrichten van de samenwerkende organisatie gaan hier sturingsvragen aan vooraf.

Sturingsvragen voor gemeenten/secretarissen

1. Hebben we zicht op informatiebeveiligingsbeleid bij alle gemeenten met wie we samenwerken?
2. Is er per organisatie een risicoanalyse gemaakt om de risico's boven tafel te krijgen?
3. Hebben we (contractuele) afspraken gemaakt over het gebruik van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als norm voor het basis-beveiligingsniveau van samenwerkingsverbanden, zo nodig inclusief tijdpad?
4. Hebben we zicht op de stand van zaken met betrekking tot de implementatie van de BIG bij de individuele gemeenten?
5. Vragen we van de samenwerkingsverbanden verantwoording over de wijze waarop zij aan de BIG (gaan) voldoen? Sluit deze verantwoording aan op onze (P&C-)cyclus?
6. Hebben we zicht op de (extra) beveiligingsmaatregelen die van ons verlangd worden door onze samenwerkingspartners en zijn die ook geïmplementeerd?

Sturingsvragen voor directeuren/vertegenwoordigers van samenwerkingsverbanden

1. Heb ik met gemeenten afspraken gemaakt over het gebruik van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als norm voor het basis beveiligingsniveau voor het samenwerkingsverband?
2. Zijn er afspraken over wie het specifieke deel van het beleid formuleert? Bijvoorbeeld het suwi-veiligheidsbeleid dat generiek is ten opzichte van het algemene informatiebeveiligingsbeleid.
3. Heeft ons samenwerkingsverband een beveiligingsplan waarin het traject voor implementatie van de maatregelen is beschreven?
4. Rapporteren en bespreken we het functioneren van de beveiliging van informatie op management- en bestuursniveau dat aansluit op de cyclus van onze opdrachtgevers?
5. Toetsen we jaarlijks binnen het samenwerkingsverband of we in control zijn op het gebied van informatieveiligheid via peer reviews, audits of self-assessments? Verantwoord ik me daarover naar gemeenten (c.q. naar degenen die verantwoordelijk zijn voor informatieveiligheid)?
6. Stel ik de werkbaarheid van het informatieveiligheidsbeleid in samenwerking met verschillende gemeenten voldoende op de agenda?

19 Stappenplan voor een veiliger gebruik van Suwinet, VNG, 2014, https://www.vng.nl/onderwerpenindex/sociale-zaken/samenwerken-op-de-arbeidsmarkt/publicaties/stappenplan-voor-een-veiliger-gebruik-van-suwi-net

7 Tot slot

In deze notitie is stilgestaan bij de vraag hoe informatieveiligheid en verantwoording hierover geborgd kan worden in intergemeentelijke samenwerkingsverbanden. Hiervoor is ook een aantal stuurvragen geformuleerd. Deze stuurvragen kunnen gebruikt worden bij een verkenning aan de bestuurstafel. Om vervolgens aan de slag te gaan, is op basis van deze informatie een aantal stappen (niet limitatief en logischerwijs volgtijdelijk) geformuleerd om informatieveiligheid van een gemeente richting een intergemeentelijke samenwerkingsverband te borgen en vice versa. Deze stappen zijn in onderstaand kader opgenomen.

Stappen borging informatieveiligheid gemeentesecretaris/directeur samenwerkingsverband

Analyseer de samenwerkingspartners

- Stel een overzicht samen van de samenwerkingsverbanden en ga na welke afspraken zijn gemaakt ten aanzien van informatieveiligheid en verantwoording hierover.

Stel het informatiebeveiligingsniveau vast

- Leg met het samenwerkingsverband vast dat het normenkader van de BIG wordt toegepast en maak afspraken over de uitvoering ervan. Bijvoorbeeld als het gaat om uitvoering geven aan een gap-analyse, incident- en crisismanagement, het continuïteitsplan, etc.

Maak afspraken over de coördinatie en afstemming

- Om dubbelwerk voor de gemeente en het samenwerkingsverband te voorkomen, moet duidelijk zijn hoe de coördinatie en afstemming is geregeld. Bijvoorbeeld als het gaat om de implementatie van maatregelen.

Leg vast hoe de verantwoording plaatsvindt

- Leg vast waarover en wanneer het samenwerkingsverband zich verantwoord over informatieveiligheid. Centraal moet de vraag staan in hoeverre het samenwerkingsverband in control is op het gebied van informatieveiligheid. Dit kan via peer reviews, audits of self-assessments.
- Spreek af dat de planning- en controlcyclus van het samenwerkingsverband aansluit op de planning- en controlcyclus van de gemeente.

Plan leer- en evaluatiemomenten

- Maak afspraken met het samenwerkingsverband over periodieke evaluatiemomenten om na te gaan hoe de afstemming en coördinatie verloopt, in hoeverre het informatiebeveiligingsbeleid werkbaar/uitvoerbaar is en of op basis van veranderingen in de interne organisatie of in de externe omgeving aanpassingen nodig zijn.

8 Verwijzingen relevante instanties

- Taskforce Bestuur en informatieveiligheid Dienstverlening (voor informatie, instrumenten en bijeenkomsten):
  http://www.taskforcebid.nl/
- Kwaliteitsinstituut Nederlandse Gemeenten (informatie)
  https://www.kinggemeenten.nl/
- Informatiebeveiligingsdienst Nederlandse Gemeenten (informatie rondom incidenten, de BIG en relevante bijeenkomsten)
  https://www.ibdgemeenten.nl/
- Vereniging Nederlandse Gemeenten
  - Dossier dienstverlening en informatiebeleid, wegwijzer informatieveiligheid, stappenplannen
    http://www.vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid
  - Wegwijzer informatieveiligheid
    http://www.vng.nl/bw/startpagina-burgemeesters-en-wethouders/wegwijzers-burger-en-recht/wegwijzer-informatieveiligheid
  - Stappenplan voor veilig gebruik Suwinet
    https://www.vng.nl/onderwerpenindex/sociale-zaken/samenwerken-op-de-arbeidsmarkt/publicaties/stappenplan-voor-een-veiliger-gebruik-van-suwi-net