# GEMEENTE BEDUM

**Commissie** : 2 februari 2017
**ABZ/ROM**
**AGENDAPUNT** : 2
**RV NUMMER**

**ONDERWERP** : Informatiebeveiliging in BMWE

**VOORSTEL** :

1. € 41.740,-- beschikbaar stellen voor de uitvoering van informatiebeveiliging BMWE in 2017;
2. deze kosten in 2017 te dekken uit de Algemene Reserve;
3. de structurele dekking van deze kosten voor de jaren 2018 en verder mee te nemen in de Voorjaarsnota 2017.

**TOELICHTING** :

**Inleiding**
Dit advies gaat over de opgave voor de naleving, toetsing en uitvoering van het informatiebeveiligingsbeleid voor de komende jaren. De aanstelling van een gezamenlijke informatiebeveiligingsfunctionaris (IBF)[1] voor de BMWE-gemeenten staat centraal.

De BMWE-colleges hechten, in navolging van de Resolutie Informatieveiligheid[2] die eind 2013 unaniem door de ledenraad van de VNG is omarmd, belang aan een zorgvuldige en veilige uitwisseling van (persoons)gegevens die goed aansluit bij de praktijk. Hier is en wordt in geïnvesteerd door de Baseline Informatiebeveiliging Gemeenten (BIG) te implementeren. Op dit moment gebeurt dit in Eemsmond onder leiding van de informatiebeveiligingsfunctionaris en in de BMW gemeenten onder leiding van een tijdelijk ingehuurde informatiebeveiligingsfunctionaris.

Met het oog op de herindeling van de BMWE gemeenten tot één gemeente, wat de vier raden onlangs bekrachtigden, bestaat de wens onder de directies van de gemeenten het thema informatiebeveiliging onder te brengen bij één gezamenlijke informatiebeveiligingsfunctionaris. In deze adviesnota wordt die wens verder uitgewerkt.

**Beleid**
De opgave op het gebied van informatiebeveiliging is binnen de BMWE-colleges al in een eerder stadium onder de aandacht geweest. Het college van Eemsmond stelde de beleidsuitgangspunten vast in april 2015 en het informatiebeveiligingsbeleid, naar verwachting, in januari 2017. Het management van Eemsmond stelde het informatiebeveiligingsbeleid reeds vast in augustus 2016.

De colleges van Bedum, De Marne en Winsum hebben het informatiebeveiligingsbeleid vastgesteld in januari/februari 2017. De beleidskaders zijn alle vier een afgeleide van het informatiebeveiligingsbeleid zoals dat is opgesteld door de Informatiebeveiligingsdienst (IBD)[3]. Dat maakt het in gezamenlijkheid uitvoeren van dit beleidsveld praktisch goed haalbaar.

In het informatiebeveiligingsplan staat nader uitgewerkt welke maatregelen er nog geïmplementeerd dienen te worden, volgens welke planning en volgordelijkheid dit geschiedt, alsmede de verantwoordelijke voor de uitvoering. De BMWE gemeenten maken bij de uitvoering reeds gebruik van hetzelfde Information Security Management System (ISMS[4]) om zodoende de maatregelen ook organisatorisch te borgen tijdens én na de implementatie.

[1] *Voor dezelfde functie wordt ook veelal de Engelse term CISO gebruikt; Chief Information Security Officer*
[2] *https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente*
[3] *De IBD is een initiatief van KING en de VNG*
[4] *Een ISMS is een management proces voor de besturing van, en verantwoording over informatiebeveiliging*

Informatiebeveiliging en privacy zijn twee kanten van dezelfde medaille. De privacy-opgave voor de BMWE gemeenten overlapt ten dele met de opgave op het gebied van informatiebeveiliging. In december 2016 is reeds besloten door de colleges van de BMWE-gemeenten tot de aanstelling van een gezamenlijke privacyfunctionaris. In dat licht bezien is het wenselijk dat de informatie-beveiligingsfunctionaris ook de 'scope' BMWE krijgt in plaats van een deel daarvan. Op deze manier wordt de samenwerking ten volle benut, zowel tussen de gemeenten als tussen beide functionarissen.

Tot slot is het hier van belang te benadrukken dat een informatiebeveiligingsfunctionaris zijn/haar werk doet vanuit een onafhankelijke positie (buiten de lijn c.q. het primaire proces). De persoon moet in staat zijn onafhankelijk te rapporteren en te adviseren over informatiebeveiliging aan het management en het bestuur.

**Uitvoering**
De coördinatie van de uitvoering van het informatiebeveiligingsbeleid ligt in handen van de informatiebeveiligingsfunctionaris. Alhoewel de verantwoordelijkheid voor de uitvoering van de maat-regelen belegd is bij het lijnmanagement, vervult de informatiebeveiligingsfunctionaris een belangrijke rol in de implementatie en het beheer van de BIG maatregelen. Het is de persoon die de BIG implementatie gemeentebreed coördineert en hierover rapporteert aan het management en het bestuur. In bijlage 1 staan de kerntaken van de informatiebeveiligingsfunctionaris opgesomd.

**Formatie**
Bij het bepalen van de benodigde formatie van de informatiebeveiligingsfunctionaris en ondersteuner wordt uitgegaan van de vuistregel zoals die wordt aangereikt door de Informatiebeveiligingsdienst: het implementeren van BIG maatregelen kost gemiddeld 16u per maatregel. Grofweg hebben de BMWE-gemeenten ieder 200 BIG maatregelen te implementeren over een periode van 2 jaar. Vier gemeenten maal 100 maatregelen per jaar vertaalt zich naar 400 x16 u = 3200 u per jaar. Afgerond komt dit neer op twee fte. Na de implementatiefase zal dit geleidelijk afnemen naar één fte. In bijlage 1 ziet u op welke taken de ondersteuner ondersteuning biedt aan de informatiebeveiligingsfunctionaris.

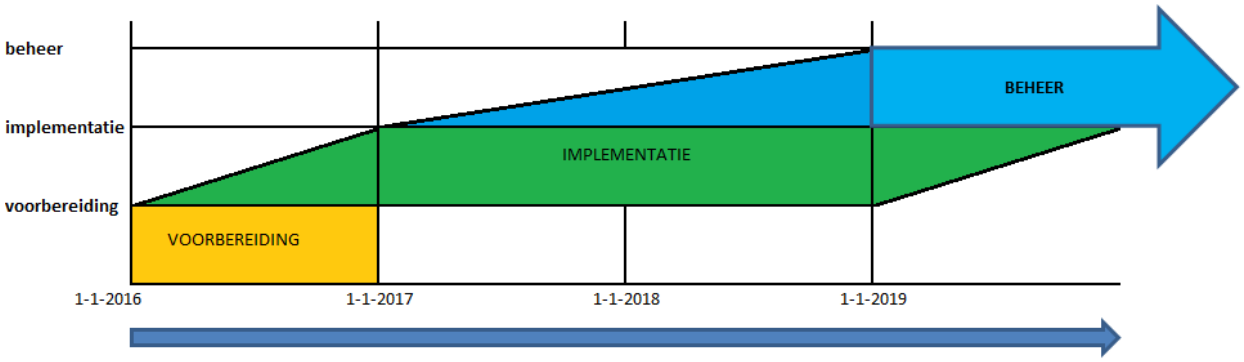
De winsten van het gezamenlijk implementeren van de BIG vertalen zich op korte termijn (tot aan de herindeling) nog niet terug om de volgende drie redenen:

1) De herindeling zal op z'n vroegst per 1 januari 2019 geeffectueerd zijn wat betekent dat de informatiebeveiligingsfunctionaris tot aan dat moment werkt voor vier afzonderlijke gemeenten met een zekere mate van inefficiëntie.
2) De implementatie van de BIG brengt veel uitvoerend werk met zich mee dat ook ten dele door de informatiebeveiligingsfunctionaris wordt uitgevoerd. Daarnaast coördineert hij/zij de implementatie van de maatregelen waarvan de uitvoering bij een VAKA deling belegd is. Daarbij is de uitgangssituatie per gemeente verschillend.
3) Binnen de BMW gemeenten is het ISMS pas recent geïmplementeerd waardoor de werkwijze in de komende periode moet worden uitgelijnd met de procedures uit dit ISMS. Daartoe zijn de eerste stappen gezet, maar deze nieuwe werkwijze zorgt echter wel voor een extra urenbelasting in de eerste jaren.

Het is daarom raadzaam de informatiebeveiligingsfunctionaris voor BMWE in ieder geval in de implementatiefase van de BIG te laten ondersteunen door een andere functionaris.

**BMW**
Om het verloop van de BIG implementatie als project overzichtelijk te houden treft u hieronder een grafische weergave aan. Begin 2016 hebben de colleges van de BMW gemeenten ingestemd met de adviesnota 'Informatiebeveiliging BMW-gemeenten'. De vier aldaar benoemde fasen komen als volgt overeen met onderstaande figuur.

| | |
|---|---|
| *voorbereiding* | fase 1 (inventariseren en analyseren) en fase 2 (afwegen en vaststellen) |
| *implementatie* | fase 3 (implementeren) |
| *beheer* | fase 4 (monitoren en controleren) |




**Eemsmond**

Het verloop van de BIG implementatie bij de gemeente Eemsmond is anders van bij de BMW gemeenten. Als één van de eerste stappen van de BIG implementatie is in Eemsmond de functie van informatie-beveiligingsfunctionaris beschreven met als belangrijkste bevoegdheid om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. De Medewerkers gegevensbeheer zijn in die functie benoemd.

Uit een onlangs uitgevoerde formatieberekening van het team gegevensbeheer is duidelijk geworden dat het aantal taken van dit team vier formatieplaatsen vereist, terwijl de formatie uit twee fte's bestaat. Een uitbreiding van formatie is daarom zeer gewenst.

De beleidsuitgangspunten zijn door het bestuur vastgesteld, de GAP-analyse is uitgevoerd en de Verklaring van Toepasselijkheid (VVT) is voorlopig vastgesteld. Het Informatiebeveiligingsbeleid is door het MT akkoord bevonden om ter vaststelling aan burgemeester en wethouders te worden voorgelegd. Verder zijn er reeds diverse procedures vastgesteld die een hoger niveau van informatiebeveiliging garanderen.

De ingestelde beveiligingscommissie werkt thans aan de voorbereiding van meerdere maatregelen in het kader van de BIG. Eén van de maatregelen die in Eemsmond hoog op de agenda staat is de uitvoering van het i-Bewustzijnsprogramma dat in oktober van dit jaar is gestart en in januari een vervolg krijgt in de vorm van een e-Learningstraject.

**Herindeling**

Het aanstellen van één gezamenlijke informatiebeveiligingsfunctionaris voor de BMWE gemeenten sorteert uitstekend voor op de herindeling. Immers, de vier gemeenten dienen aan exact dezelfde eisen te voldoen en door in de aanloop naar de herindeling al één informatiebeveiligingsfunctionaris te hebben worden beleid, processen en, waar mogelijk, applicaties al zoveel mogelijk uitgelijnd zodat er één werkwijze gaat ontstaan. Kortom, een gezamenlijke informatiebeveiligingsfunctionaris versterkt, en geeft (alvast) concreet invulling aan de steeds nauwere samenwerking met als stip aan de horizon de herindeling.

**Beoogd resultaat**

Alleen met het aanstellen van één informatiebeveiligingsfunctionaris voor de BMWE gemeenten kan, in de aanloop naar de herindeling, het volgende beoogde resultaat worden behaald:

- Een veilige gegevensverwerking en –uitwisseling binnen de BMWE gemeenten door een succesvolle implementatie van de Baseline Informatiebeveiliging Gemeenten.
- Blijvende monitoring en controle op het stelsel van maatregelen met behulp van het Information Security Management System (ISMS).
- Structureel en blijvend aandacht en bewustzijn voor informatiebeveiliging (en privacy) op alle levels binnen de gemeenten.
- Integrale en professionele verantwoording conform de planning & control cyclus.

**Financiën**
In de begrotingen 2017 van de BMWE gemeenten is vooralsnog geen post opgenomen voor de invulling van de informatiebeveiligingsfunctionaris. Binnen Eemsmond wordt op dit moment de functie informatiebeveiligingsfunctionaris ingevuld door twee medewerkers van de afdeling gegevensbeheer. Om die reden is er in de begroting van Eemsmond eveneens geen post opgenomen voor de informatie-beveiligingsfunctionaris.

Binnen BMWE wordt gebruik gemaakt van het functiewaarderingssysteem HR21[5] van de VNG. P&O van BMW heeft de functiebeschrijving van de informatiebeveiligingsfunctionaris voor inpassing in het HR21 model voorgelegd aan het bureau BuitenhekPlus/Leeuwendaal. Op basis van hun advies en verdere inpassing in het HR21 model bedragen de formatiekosten maximaal € 73.000,-- voor de informatie-beveiligingsfunctionaris en maximaal € 60.000,-- voor de ondersteuner. Beide bedragen zijn voor de BMWE gemeenten samen, en in de gemeentelijke begrotingen 2017 is geen structurele dekking opgenomen voor deze beide functies.
Hieronder een overzicht van de te ramen structurele bedragen voor de formatie van beide functionarissen. De verdeelsleutel is gebaseerd op het aantal inwoners per 1-1-2016 (Bedum 20,87%, De Marne 20,21%, Winsum 27,28%, Eemsmond 31,64%).

| **Formatiekosten voor informatiebeveiligingsfunctionaris & ondersteuner voor BMWE** | | | |
|---|---|---|---|
| Gemeente | Huidige dekking | Benodigde dekking | Nog te ramen |
| **Bedum** | € 0,- | € 27.757,10 | € 27.757,10 |
| **De Marne** | € 0,- | € 26.879,30 | € 26.879,30 |
| **Winsum** | € 0,- | € 36.282,40 | € 36.282,40 |
| **Eemsmond** | € 0,- | € 42.081,20 | € 42.081,20 |
| **Totaal** | **€ 0,-** | **€ 133.000,--** | **€ 133.000,--** |

Daarnaast heeft de informatiebeveiligingsfunctionaris een eigen budget nodig om goed invulling te geven aan zijn/haar verantwoordelijkheden. Uit dit budget worden zaken als bewustwording, penetratietesten, audits en tooling bekostigd. Dit bedrag zal na 1-1-2019 aanzienlijk lager zijn omdat de verantwoordingslast op dat moment van vier naar één gemeente teruggaat. Na afronding van de implementatie wordt heroverwogen of de informatiebeveiligingsfunctionaris een eigen budget dient te behouden, of dat ook dit budget wordt ondergebracht bij de diverse vakafdelingen. Tot slot zijn aan het eerder genoemde ISMS van Segment ook jaarlijkse kosten verbonden.

Een overzicht van de jaarlijkse, structurele kosten voor informatiebeveiliging (IB).

| *(bedragen per jaar)* | **BMWE** | **Bedum** | **De Marne** | **Winsum** | **Eemsmond** |
|---|---|---|---|---|---|
| ISMS Segment | € 19.800,-- | € 4.950,-- | € 4.950,-- | € 4.950,-- | € 4.950,-- |
| Budget IB | € 60.000,-- | € 15.000,-- | € 15.000,-- | € 15.000,-- | € 15.000,-- |
| Formatiekosten | € 133.000,-- | € 27.757,10 | € 26.879,30 | € 36.282,40 | € 42.081,20 |
| Totale kosten | € 212.800,-- | € 47.707,10 | € 46.829,30 | € 56.232,40 | € 62.031,20 |
| Aanwezige dekking | € 22.850,-- | € 5.967,-- | € 5.967,-- | € 5.967,-- | € 4.950,-- |
| **Nog te ramen** | **€ 189.950,-** | **€ 41.740,10** | **€ 40.862,30** | **€ 50.265,40** | **€ 57.081,20** |

Voor de kosten in 2017 worden de kosten geraamd middels een begrotingswijziging, zodat de uitvoering op korte termijn plaats kan vinden. Dekking voor dit jaar kan plaatsvinden uit de algemene reserve. Voor wat betreft de structurele lasten van 2018 e.v. zullen we de kosten meenemen in de kaderstelling bij de voorjaarsnota 2017.

Belangrijk
De kosten in uren en euro's voor het uitvoeren van de maatregelen zelf, binnen de diverse vakafdelingen, zijn niet opgenomen in bovenstaand overzicht.

[5] http://www.hr21.nl/

Dit zijn immers kosten die terug dienen te komen in de capaciteitsplanningen en begrotingen van de betreffende vakafdelingen. In deze nota wordt dan ook geen dekking gevraagd voor de kosten van de uitvoering van de maatregelen zelf.

**Samenvatting**
Om uitvoering te geven aan het voorliggend voorstel dienen de BMWE gemeenten een aantal concrete stappen te nemen:

- de aanstelling van één informatiebeveiligingsfunctionaris voor de BMWE gemeenten;
- de aanstelling van een ondersteuner voor de informatiebeveiligingsfunctionaris *tijdens de implementatiefase* van de Baseline Informatiebeveiliging Gemeenten (BIG);
- de informatiebeveiligingsfunctionaris te doen beschikken over een eigen budget voor informatie-beveiliging en
- de informatiebeveiligingsfunctionaris te ondersteuning met een ISMS-applicatie.

**Voorstel**
Om bovenstaande te bereiken vraagt het college de raad:

- € 41.740,- beschikbaar te stellen voor de uitvoering van informatiebeveiliging BMWE in 2017;
- deze kosten in 2017 te dekken uit de Algemene Reserve;
- een voorstel voor de structurele dekking van deze kosten voor de jaren 2018 e.v. mee te nemen in de kaderstelling bij de Voorjaarsnota 2017.

Bedum, 24 januari 2017

Burgemeester en wethouders van de gemeente Bedum,

| | |
|---|---|
| De secretaris, | De loco-burgemeester, |
| R. Wiltjer | M. van Dijk |