GEMEENTEBARENDRECHT | Gemeente Albrandswaard | RIDDERKERK GEMEENTE RIDDERKERK

Aan het College van Burgemeester en Wethouders van Ridderkerk

| | | | |
|---|---|---|---|
| Uw brief van: | - | Kenmerk: | |
| Uw kenmerk: | - | Contactpersoon: | R. van Bochove |
| Bijlage(n): | 1 | Afdeling: | Directie |
| Onderwerp: | Zienswijze op begrotingswijziging GR BAR-organisatie over Informatieveiligheid en Privacy | Doorkiesnummer: | |
| | | Datum: | |

Geachte collegeleden,

Wij nodigen u uit kennis te nemen van ons besluit inzake de noodzaak om extra maatregelen te nemen op het gebied van informatieveiligheid en privacy. Daarbij vragen wij u om de noodzakelijke begrotingswijziging door te geleiden naar de gemeenteraad voor de zienswijzeprocedure.

**Aanleiding**
In opdracht van het dagelijks bestuur van de BAR-organisatie is in 2021 een Breed onderzoek uitgevoerd naar informatiebeveiliging en privacy. Hierbij is een analyse gemaakt van hoe de gemeenten Ridderkerk, Barendrecht en Albrandswaard er voor staan en wat er structureel nodig is in de komende jaren. Deze opdracht is mede gegeven op basis van het Rekenkamer onderzoek in Ridderkerk naar de implementatie van de AVG en het onderzoek van Concerncontrol in Barendrecht en Albrandswaard naar de implementatie van de AVG. Het Breed onderzoek is nu klaar.

De uitkomsten van het onderzoek zijn besproken in het Dagelijks Bestuur van de BAR-organisatie. Wij hebben een besluit genomen over de noodzaak van aanvullende maatregelen en de daarbij behorende extra middelen. De daarvoor benodigde begrotingswijziging wordt via uw college met een zienswijzeprocedure aan de raad aangeboden. Hierna kan het Algemeen Bestuur van de BAR-organisatie, met inachtneming van de uitgebrachte zienswijzen, een besluit nemen.

**Wat ging vooraf**

1. Eind 2020 is door het DB een uitvoeringsplan vastgesteld op basis van het Rekenkameronderzoek Ridderkerk en een tweetal onderzoeken door Concerncontrol in Barendrecht en Albrandswaard naar de implementatie van de AVG. Voor dat uitvoeringsplan is voor 2021 incidenteel € 200.000,- beschikbaar gesteld om een aantal pilots en een breed onderzoek uit te voeren.

2. Met de vaststelling van het uitvoeringsplan heeft het DB tevens verzocht om een breed onderzoek te doen naar wat er structureel nodig is op het gebied van informatiebeveiliging en privacy. Op te leveren eind 2021.

3. In de zomer van 2021 hebben de drie portefeuillehouders bedrijfsvoering toestemming gegeven om incidenteel € 100.000,- uit te geven om een aantal acuut benodigde maatregelen te nemen op het gebied van cybersecurity. De financiële verantwoording van deze incidentele kosten loopt via het rekeningresultaat van de jaarrekening van onze organisatie.

4. In het laatste kwartaal van 2021 is binnen de formatie van de BAR-organisatie extra ingehuurd om de sterk toegenomen taken op het gebied van dataveiligheid en privacy op te kunnen vangen.

5. In het afgelopen jaar is daarnaast de noodzaak om meer maatregelen te nemen op het gebied van informatiebeveiliging en privacy toegenomen. Er is sprake van een groeiende dreiging op het gebied

van cyber aanvallen. Er zijn steeds meer concrete voorvallen om ons heen en zeer recent ook een tweetal aanvallen op ons eigen netwerk. Deze aanvallen hebben we kunnen pareren door de genomen maatregelen in de zomer. De toezichthouders zijn ook actiever geworden en geven gemeenten extra aansporingen om aanvullende maatregelen te nemen. Onder andere vanuit de VNG en het nationaal cybersecurity center van het Rijk.

**Inhoudelijke onderbouwing**

*De ontwikkelingen op het gebied van informatieveiligheid en privacy gaan snel. Om de basis dienstverlening en de bedrijfsvoering te kunnen blijven garanderen is het noodzakelijk om de formatie op het gebied van informatieveiligheid en privacy in onze organisatie in overeenstemming te brengen met het dreigingsniveau. Daarom heeft het DB dit besluit genomen.*

*Waar komen we vandaan*
Na de start van de BAR-organisatie in 2014 is gewerkt aan het op poten zetten van de organisatie op het gebied van informatieveiligheid en privacy. Destijds is er gekozen voor een efficiënte formatieve bemensing. Met een Privacy Officer (PO), een Chief Information Security Officer (Ciso) en een inhuur constructie van een dag per week voor een Functionaris Gegevensbescherming (FG). Door de jaren heen heeft het onderwerp informatieveiligheid en privacy aan gewicht gewonnen.

*Reële dreiging en aanvullende stappen gezet in de organisatie*
In de afgelopen twee jaar hebben we extra stappen gezet in de organisatie. We zijn gestart met een intern cyber team. Het zogenaamde CERT (Computer Emergency Response Team). Met dit team zijn we in staat om acuut te handelen bij potentiele beveiligingsrisico's waardoor we als organisatie aan slagkracht hebben gewonnen. Op advies van het CERT hebben we afgelopen zomer geïnvesteerd in zogenaamde logging en monitoring software. Hiermee kunnen we verdachte activiteiten op ons netwerk detecteren. Een externe specialist ondersteunt ons bij de analyse van deze gegevens en adviseert over de opvolging. Dit heeft direct een positief effect gehad. In november en december 2021 hebben we twee concrete cyber aanvallen vroegtijdig weten te detecteren en de benodigde beheer maatregelen kunnen nemen. Dit is een belangrijk succes. En tegelijkertijd maakt het ook zichtbaar dat de risico's en dreiging reëel zijn. Naast de instelling van het CERT en de incidenteel verbeterde monitoring en logging is ook een aantal aanvullende maatregelen genomen en/of in voorbereiding. Het is zeer noodzakelijk om deze maatregelen structureel in te bedden in onze organisatie.

*Grenzen van wat we binnen de huidige bezetting kunnen zijn bereikt*
Uit het bovenstaande valt op te maken dat we in de afgelopen jaren een goede ontwikkeling hebben doorgemaakt. En dat is ook nodig. Het belang van deugdelijke informatiebeveiliging en privacy waarborgen is de laatste drie jaar enorm toegenomen. Het externe dreigingsbeeld is verslechterd en we verwerken steeds meer privacy gevoelige informatie en koppelen steeds meer data. De afgelopen twee jaar is dan ook steeds meer duidelijk geworden dat onze huidige manier van werken niet meer toereikend is. Dit is deels geconstateerd door de Rekenkamer in Ridderkerk en door concern control. Daarbovenop sporen de VNG (zie bijlage) en de Informatie Beveiliging Dienst (zie bijlage) van het Rijk gemeenten aan om meer maatregelen te nemen. De incidenten in de wereld om ons heen nemen in rap tempo toe. Bijna wekelijks zijn er inmiddels wel voorbeelden van cyber aanvallen op organisaties en bedrijven, ook bij onze eigen BAR-organisatie zoals eerder in dit voorstel staat beschreven. Mede op basis daarvan is een brede analyse uitgevoerd naar waar onze drie gemeenten staan op het gebied van informatieveiligheid en privacy en wat er nodig is in de komende jaren. Op basis van deze brede extern uitgevoerde analyse wordt nu een begrotingswijziging voor een zienswijze aangeboden.

Dat er een groot risico bestond op aanvullende maatregelen werd eerder ook beschreven in de paragraaf weerstandsvermogen in de begroting. Het ICT (beveiligings)risico is daarbij als hoogste risico opgenomen in de risico top 10.

*Uit het onderzoek blijkt dat het noodzakelijk is de formatie op het vlak van informatieveiligheid en privacy te versterken. Waarbij het voorstel is om de formatie op het niveau te brengen van gemeentelijke organisaties met een vergelijkbaar aantal inwoners. Hierdoor zijn we beter in staat om onze risico's te beheersen en aantoonbaar te voldoen aan het wettelijke kader.*

*Centrale formatie versus de decentrale formatie*
Het besluit van het DB is om te starten met de optie 'niveau gemeentelijke organisatie met vergelijkbaar aantal inwoners'. Daarmee brengen we de huidige krappe formatie op het vlak van informatieveiligheid en privacy in de organisatie op basisniveau. Lees, de omvang die minimaal nodig is om de basistaken uit te kunnen voeren. Te kunnen voldoen aan de AVG en de BIO. En op basis van een goede risicoafweging maatregelen te kunnen nemen indien noodzakelijk. Vergelijkbaar met andere organisaties van onze

omvang. De huidige werkpraktijk laat zien dat dit echt noodzakelijk is. De bedrijfsvoering staat onder druk. Er is in 2021 niet voor niets in twee etappes tijdelijk geld beschikbaar gesteld. En we zijn genoodzaakt om fors extra in te huren om lopende vraagstukken weg te werken en op te lossen.

Hierbij is het van belang te schetsen dat het budgettaire gevolg van deze keuze in een bandbreedte zit waarbij we nu het basisscenario als uitgangspunt nemen. Het is best mogelijk dat het op termijn noodzakelijk is om verder te groeien. Het thema informatieveiligheid en privacy is namelijk enorm in beweging. De ontwikkelingen gaan snel. Het is dan ook niet volledig te voorspellen wat er in de komende jaren nog meer nodig is. Maar de uitkomsten van het onderzoek maken in elk geval duidelijk dat een forse investering nu noodzakelijk is. De bandbreedte is hieronder in tabel vorm weergegeven waarbij de optie drie afzonderlijke gemeenten ter vergelijking is weergegeven om de opties in perspectief te kunnen plaatsen.

| **Optie** | **FTE** | **Bestaande formatie** | **Aanvullende benodigde formatie** | **Extra middelen** |
|---|---|---|---|---|
| Niveau gemeentelijke organisaties met vergelijkbaar aantal inwoners | 7 totaal | 2.2 fte | 4,8 fte (waarvan 2 fte decentraal) | € 432.000 (minimale bandbreedte) |
| Optimale optie | 10 totaal | 2,2 fte | 7,8 fte | € 702.000 (maximale bandbreedte) |
| Drie afzonderlijke gemeenten (ter vergelijking) | 11,5 totaal | 2,2 fte | 9,3 fte | € 837.000 |

Deze tabel geeft inzicht in de bandbreedte van € 432.000 - € 702.000.
Bij de opties is het totaal aantal benodigde fte's weergegeven. De geraamde bedragen gaan echter over minder fte's. Immers een deel van de formatie hebben we al. Dus het geraamde bedrag gaat over de nog toe te voegen formatie.

*Het is waarschijnlijk dat uit een nadere inventarisatie blijkt dat er nog aanvullende middelen nodig zijn.*

Het nu genomen besluit voorziet in het op orde brengen van een deel van de centrale formatie voor informatiebeveiliging en privacy en in het toevoegen van formatie voor de decentrale clusters Veiligheid en Maatschappij. Dit in de vorm van onder andere een decentrale Information Security Officier voor de clusters Veiligheid en het Sociaal Domein. Immers, daar vinden de meest risicovolle gegevensverwerkingen plaats. Het is waarschijnlijk dat er nog meer (decentrale) formatie noodzakelijk is. Bijvoorbeeld extra kwaliteitsbeheer in de werkprocessen waar risicovolle gegevensverwerkingen plaatsvinden en op het gebied van applicatiebeheer.

Met het structureel inrichten van de nu gevraagde formatie kan komend jaar een nog scherper inzicht worden gecreëerd in wat er nog meer nodig is, inclusief een goede risico-inventarisatie. Welke risico's bestuurlijk wel of niet acceptabel worden geacht is bepalend voor het niveau van aanvullende investeringen.

*Concreet uitvoeringsplan*
Na besluitvorming wordt gestart met het maken van een concreet uitvoeringsplan. Met mijlpalen en concreet te realiseren acties voorzien van een planning. Hiermee kan periodiek aan de stuurgroep, de directie en het bestuur gerapporteerd worden over de voortgang. Bij dit uitvoeringsplan hoort ook de exacte invulling van de aanvullende formatie.

**Financiële informatie**
Voor de verdeling van de kosten wordt de standaard verdeelsleutel gebruikt. Met daarbij de volgende structurele financiële effecten.

| **Budgettair vraagstuk** | **B A R totaal** | **Barendrecht** | **Albrandswaard** | **Ridderkerk** |
|---|---|---|---|---|
| Optie niveau gemeentelijke organisatie met vergelijkbaar aantal inwoners | 432.000 | 168.264 | 87.869 | 175.867 |
| Voortzetten cyber security maatregelen | 100.000 | 38.950 | 20.340 | 40.710 |
| **Totaal** | **532.000** | **207.214** | **108.209** | **216.577** |

**Indienen zienswijze**
Wij verzoeken u een eventuele zienswijze voor vrijdag 25 februari 12:00 uur in te dienen. De behandeling van deze begrotingswijziging van onze GR BAR-organisatie in het algemeen bestuur staat geagendeerd voor 8 maart 2022.

Hoogachtend,
het dagelijks bestuur van de GR BAR-organisatie,

de secretaris,

drs. Henk Klaucke

de voorzitter,

drs. Jolanda de Witte

Bijlagen:
- rapport Breed onderzoek Informatiebeveiliging en privacy
- college/raadsvoorstel
- concept zienswijze raad