



raadsmededeling

zaak/onderwerp Z-15-07149 / Informatieveiligheid/Gegevensbescherming/Visitatiecommissie
portefeuillehouder M.A. den Boer
team Bedrijfsondersteuning
opgesteld door M. Miggels
datum/nr 29 maart 2016 / CB-16-1560



Geachte raad,

Omdat er in korte tijd verschillende besluiten zijn genomen op het gebied van informatieveiligheid en gegevensbescherming, willen wij u over deze onderwerpen informeren. Dit sluit tevens aan op uw wens om, naar aanleiding van het recente datalek alsmede het inspectieonderzoek Suwi, over beide onderwerpen geïnformeerd te worden.

Informatieveiligheid

In maart 2013 is het Statuut Informatiebeveiliging voor de gemeenten Oegstgeest, Leiden, Leiderdorp, Zoeterwoude en Servicepunt71 vastgesteld. Hierin worden uitgangspunten benoemd met betrekking tot de organisatie van informatieveiligheid en enkele beleidsuitgangspunten met betrekking tot informatieveiligheid.

In mei 2013 is de Baseline informatiebeveiliging Nederlandse gemeenten (BIG) ontwikkeld door VNG en KING. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de veiligheid van informatie binnen gemeentelijke organisaties. Bij het buitengewone VNG ledencongres (29 november 2013) hebben de leden een resolutie aangenomen die van de gemeenten vraagt informatieveiligheid bestuurlijk en organisatorisch te borgen, de Baseline Informatiebeveiliging voor Nederlandse Gemeenten als standaard te hanteren en informatieveiligheid transparant te maken voor burgers, bedrijven en ketenpartners.

Vanuit de visie 'Digitale overheid 2017' van minister Plasterk moet de overheid in 2017 volledig digitaal zijn wat haar dienstverlening betreft¹. Uiteraard mag hierbij het onderwerp informatiebeveiliging niet ontbreken. Om de informatie binnen gemeenten zo goed als mogelijk beveiligd te hebben, is de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) een goede start. Er is geen exacte einddatum gekoppeld aan de implementatie van de BIG maar deze wordt gerelateerd aan de digitale overheid 2017. Gemeente Oegstgeest houdt, net als de regiogemeenten, deze planning aan voor wat betreft de informatieveiligheid.

Gemeente Oegstgeest hanteert deze nieuwe gemeente standaard (BIG) als uitgangspunt bij de inrichting van de gemeentebrede informatieveiligheid. De ambitie is om in het tweede kwartaal van 2016 één regionaal gedragen informatieveiligheidsbeleid vast te stellen voor de gemeenten Leiderdorp, Leiden, Oegstgeest, Zoeterwoude en Servicepunt71, op basis van deze Baseline. Daarnaast wordt ook op alle mogelijke aspecten van Informatieveiligheid de samenwerking gezocht als dat kan.

Om echter binnen een kort tijdsbestek al met de implementatie van de Baseline te kunnen starten, kiest Oegstgeest ervoor tussentijds dit Governance addendum toe te voegen aan het huidige Statuut. In dit addendum wordt op basis van de BIG en het reeds vastgestelde statuut de beveiligingsorganisatie en governance (besturing) van de informatieveiligheid vastgesteld. Dit betekent dat de rollen worden ingevuld, de interne informatieveiligheidsoverleggen binnen de gemeente Oegstgeest worden beschreven en de uitgangspunten ten aanzien van de incidentenprocedure worden beschreven.

De Governance en Incidentenprocedure is op 29 maart 2016 vastgesteld.

¹ Mits de beschikbare, landelijke, randvoorwaarden hiervoor beschikbaar zijn.

Gegevensbescherming

Ter kennisname bieden wij u tevens het vastgestelde beleid Gegevensbescherming aan. De sterke digitalisering van de samenleving zorgt ervoor dat het op een zorgvuldige manier verwerken van persoonsgegevens én het bewustzijn hiervan een steeds belangrijker onderwerp is binnen de organisatie. Het uitdragen en uitvoeren van het beleid draagt bij aan deze bewustwording.

De extra urgentie en behoefte aan richtlijnen voor het juist verwerken van persoonsgegevens ontstond door de veranderende taken in het sociaal domein. Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. Er moet voorkomen worden dat er onnodige of te vergaande inbreuken worden gemaakt. Het ambtelijk vooroverleg 3D heeft hierom in 2015 het initiatief genomen om beleid te laten opstellen in samenwerking met de Leidse regio gemeenten. Binnen deze gemeentes is afgesproken dat het beleid begin 2016 door de colleges is vastgesteld en de gemeenteraden zijn geïnformeerd.

De verwerking van persoonsgegevens vindt plaats in elk onderdeel van de organisatie, het beleid is daarom van toepassing voor de gehele organisatie. Het is een uitwerking van de Wet Bescherming Persoonsgegevens (Wbp) en de Meldplicht Datalekken. Er zijn ook aspecten in opgenomen vanuit de EU Algemene Verordening Gegevensbescherming (Avg) die naar verwachting per 2018 zal ingaan, zodat hier alvast op wordt voorbereid.

De maatregelen die opgenomen zijn, worden uitgewerkt in een uitvoeringsplan. Dit proces is, los van de vaststelling van het beleid, inmiddels al in volle gang én wordt daar waar mogelijk in samenwerking met de regio gemeenten opgepakt. Met ingang van 2016 nemen wij in de programmabegroting, een passage op over beleid gegevensbescherming. Als voorbereiding op de Avg wordt het beleid gegevensbescherming elk jaar geauditeerd. Elke twee jaar zal het beleid gegevensbescherming worden geëvalueerd en waar nodig bijgesteld.

Dit beleid is op 29 maart 2016 vastgesteld.

Verslag Visitatiecommissie

Naar aanleiding van de resolutie die in november 2013 op de Buitengewone Algemene Ledenvergadering van de VNG werd aangenomen, is een visitatiecommissie opgericht. Deze visitatiecommissie zou moeten toetsen of de 'verplichtende zelfregulering' voldoende werkt en of gemeenten voldoen aan de basisnormen die zijn vastgelegd in de BIG, de Baseline Informatiebeveiliging Gemeenten. Op 17 februari heeft de commissie Oegstgeest bezocht. Het verslag van dit gesprek treft u hierbij aan. In het verslag is door de commissie per hoofdthema een analyse gedaan van de besproken situatie in Oegstgeest. Het verslag is geordend langs de hoofdthema's van het gesprek:

- Digitalisering in het algemeen
- Besef van het belang om te werken aan informatieveiligheid
- Formele positionering van informatieveiligheid in de organisatie
- Daadwerkelijk uitvoeren van beleid en daadwerkelijk leren
- Extern leren en participeren in netwerken

De commissie concludeert dat de gemeente Oegstgeest zich het belang van informatieveiligheid voor haar dienstverlening beseft. Daarbij viel de Commissie specifiek positief op dat Oegstgeest op bestuurlijk en topambtelijk niveau doordrongen is van het belang van informatieveiligheid en gemotiveerd is om stappen voorwaarts te maken. Tegelijkertijd zag de Commissie dat Oegstgeest;

- zich realiseert dat niet alle stappen tegelijk genomen kunnen worden en de gemeente werkt aan een uitvoerbaar programma dat op korte termijn eerste resultaten oplevert,
- daarbij nadrukkelijk aandacht heeft voor de verbinding tussen informatieveiligheid als onderdeel van het primaire proces en het perspectief voor ogen heeft dat informatieveiligheid waarde toevoegt aan de dienstverlening. De Commissie gaf aan ook voor deze benadering te staan.

Tot slot;

Wij zijn ons er van bewust dat uitvoering geven aan alle aspecten rond informatieveiligheid en gegevensbescherming onderdeel zijn van een continue proces dat doorlopend aandacht vereist. Wij hebben er vertrouwen in dat dit binnen de organisatie goed geborgd wordt.

Burgemeester en wethouders van Oegstgeest



de secretaris
H.A. Leegstra



de burgemeester
E.R. Jaensch

Bijlagen: Governance en Incidentenprocedure Oegstgeest volgens Baseline (addendum) v1.00
Beleid Gegevensbescherming
Aanbiedingsbrief en verslag Visitatiecommissie

