Raadsvoorstel gemeente Ooststellingwerf

Commissievergadering

Onderwerp	:	Rapportage informatieveiligheid en privacy 2018
Portefeuillehouder/Teamleider	:	Harry Oosterman/Wim Waanders
Zaaknummer	:	0085-AZK-59199

Voorstel

Kennis te nemen van de rapportage informatieveiligheid en privacy 2018.

Inleiding

Waarom ENSIA?

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Gemeenten roepen in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. Dit vormde de aanleiding voor de start van het project ENSIA.

Wat is ENSIA?

Informatieveiligheid en privacy hebben een belangrijke plaats op de gemeentelijke agenda. Zorgvuldig omgaan met informatie van burgers staat bij ons hoog in het vaandel. Dat geldt voor elke afdeling van onze gemeente. Het adequaat inrichten van verantwoordingsprocessen is daarbij essentieel. Zo blijft informatieveiligheid en privacy van burgers gewaarborgd.

Over 2018 verantwoorden wij ons over de kwaliteit van de informatieveiligheid van diverse informatiesystemen met een uniforme Audit systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). Of we voldoen aan deze Baseline is getoetst door middel van een zelfevaluatie.

Voor het jaar 2018 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit de zelfevaluatie en is getoetst door een IT-auditor.

De Collegeverklaring ENSIA 2018 omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.0).

Uit de Collegeverklaring ENSIA blijkt dat aan alle normen m.b.t. de DigiD-aansluitingen en SUWI wordt voldaan. De aanbevelingen welke zijn opgenomen in de onderliggende rapportages van bevindingen zijn derhalve niet dwingend van aard en zullen met de verantwoordelijken worden besproken waarbij op basis van risico-inschatting een afweging zal worden gemaakt of het noodzakelijk is eventuele maatregelen te treffen.

Over het totaalbeeld en de status van informatieveiligheid en privacy van de gemeente verantwoordt de organisatie zich via deze separate rapportage aan de raad met de collegeverklaring als bijlage. Deze jaarrapportage bevat de ontwikkelingen, activiteiten, incidenten en risico's met betrekking tot de onderwerpen informatieveiligheid en privacy bij de gemeente Ooststellingwerf over het jaar 2018. De verantwoording aan de raad dient voor 15 juli 2019 plaats te vinden. In de bijgaande infographic is het verantwoordingsproces in hoofdlijnen weergegeven. Zo krijgt het gemeentebestuur meer zicht op de

informatieveiligheid en is ze beter in staat om keuzes te maken in het informatieveiligheidsbeleid van de gemeente.

Samenvatting en conclusie status informatiebeveiliging en privacy:

Per 25 mei 2018 voldoet de gemeente aan de minimale gestelde 6 maatregelen in het kader van de privacywetgeving, de AVG, weergegeven in hoofdstuk 5..

Hieronder een overzicht van de behaalde resultaten op de verschillende onderdelen waarover in het kader van informatiebeveiliging verantwoording moet worden afgelegd aan de toezichthouders:

Suwinet en DigiD:
De scope van de IT-audit in 2018 heeft betrekking op DigiD en SUWI. Aan alle normen m.b.t. de DigiD-aansluitingen en SUWI wordt voldaan. Dit blijkt uit de Collegeverklaring ENSIA, onafhankelijk getoetst door een IT-auditor.

BAG:
Onze gemeente heeft de administratieve inrichting van de BAG in de uitvoering structureel goed geborgd. Met een score van 90 % wordt ruimschoots voldaan aan de minimale norm van 75%. Op het onderdeel tijdigheid voldoet de gemeente niet volledig aan de specifiek gestelde beveiligingsmaatregelen, mede doordat de normen in vergelijking met het jaar 2017 zijn aangescherpt. Vanaf september 2018 zijn er acties ondernomen om er op toe te zien dat de werkafspraken correct worden nageleefd.

BGT:
Ook blijkt dat onze gemeente de uitvoering van het beheer en de kwaliteit van de BGT beheerst en waarborgt. De BGT is een vrij recente taak en zal zich door ontwikkelen tot het jaar 2020. Een maximale score hier is daarom logischerwijs nog niet mogelijk, maar zijn ten opzichte van het vorig jaar zichtbaar verbeteringen doorgevoerd. Met een score van 93% wordt ruimschoots voldaan aan de minimale norm van 75 %.

BRO:
Met ingang van het jaar 2018 is de uitvoer van een eventuele zelfevaluatie Basisregistratie Ondergrond (BRO) nieuw. Binnen onze gemeente hebben we op dit onderdeel in 2018 echter nog geen stappen ondernomen. Het jaar 2018 is een proefjaar, de uitvoer van de zelfevaluatie is derhalve niet verplicht. Formeel is deze taak nog niet belegd, dit zal in de loop van 2019 plaatsvinden. Met ingang van het jaar 2020 zal ook verantwoording worden afgelegd over de BRO.

BRP:
Uit de uitgevoerde zelfevaluatie blijkt dat onze gemeente met een totaalscore van 94% voldoende scoort op de inrichting, de werking en de beveiliging van de basisregistratie Personen. Onze gemeente voldoet daarmee aan de wettelijke norm van 90%.

PNIK:
Uit de uitgevoerde zelfevaluatie blijkt dat onze gemeente met een totaalscore van 93,7 % goed scoort op kwaliteit en veiligheid van het aanvraag- en uitgifteproces Paspoorten en Nederlandse identiteitskaarten. Onze gemeente voldoet daarmee aan de wettelijke norm van 90%.

Conclusie:
Onze gemeente kan zichtbaar aantonen goede resultaten te hebben behaald over de status van informatiebeveiliging over het jaar 2018 en voldoet aan de minimale gestelde eisen in het kader van de AVG.

Verklaring van Toepasselijkheid (VVT)
De gemeente heeft informatiebeveiligingsbeleid, vastgesteld d.d. 7 februari 2017, gebaseerd op de BIG. Er heeft in dat kader destijds een GAP- en impactanalyse plaatsgevonden op de 133 beheersmaatregelen van de BIG met als resultaat dat we inzicht hebben in de status van informatiebeveiliging, actiehouders en planning. De uitkomsten hiervan worden te zijner tijd, na afloop van het verantwoordingsjaar 2018, rond me/juni 2019 geactualiseerd en verwerkt in de zogenaamde Verklaring van Toepasselijkheid (VVT) en onderliggend jaarplan.

Met het vaststellen van de VVT doet het college een uitspraak welke beveiligingsmaatregelen we gaan nemen en welke maatregelen we bewust/weloverwogen niet nemen (aanvaardbaar risico). De concrete maatregelen worden vervolgens verwerkt in een informatiebeveiligingsplan, gecombineerd met de resultaten uit de zelfevaluaties in het kader van ENSIA die gebaseerd is op de BIG. De voorliggende rapportage Informatieveiligheid en Privacy geeft een totaalbeeld over de behaalde resultaten in 2018.

De Verklaring van Toepasselijkheid geeft zeer gedetailleerd inzicht - op het niveau van 303 beveiligingsmaatregelen - in de technische en organisatorische getroffen beveiligingsmaatregelen en daarmee inzicht in de gehele mate van beveiliging binnen onze gemeente. Het openbaar maken van deze gegevens kan echter de veiligheid van de gemeente Ooststellingwerf en onze inwoners schaden. Ook in het kader van de Wet openbaarheid bestuur (WOB) kunnen wij om dezelfde reden ons beroepen op de zogenaamde absolute uitzonderingsgrond (art. 10). Het inbrengen van de Verklaring van Toepasselijkheid kan alleen met geheim verklaring.

In de loop van 2019 zal er wederom een GAP- en impactanalyse plaatsvinden, echter nu gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO, zie in het jaarrapport 4.2 onder ontwikkelingen). De BIO bestaat uit een verplichte set aan te treffen maatregelen. Voor maatregelen die niet voor onze gemeente van toepassing zijn moet een risicobehandelplan worden opgemaakt (hiermee ontstaat dan op een totaal andere wijze een nieuwe Verklaring van Toepasselijkheid).

Conclusie:
Vorig jaar is bij de bespreking van de rapportage informatieveiligheid en privacy 2017 toegezegd de Verklaring van Toepasselijkheid (VVT) ter inzage in de raad te brengen. Stukken in de raad zijn echter, conform artikel 19 van de Gemeentewet, openbaar, dit is op basis van bovenstaande niet wenselijk. Het inbrengen van de Verklaring van Toepasselijkheid kan alleen met geheim verklaring. Uw raad wordt middels de voorliggende rapportage op de hoogte gesteld van de behaalde resultaten op het gebied van informatiebeveiliging en privacy en maakt tevens onderdeel uit van de P&C-cyclus, als onderwerp opgenomen in de paragraaf Bedrijfsvoering.

Beoogd effect
Het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG.

Argumenten
Over 2018 dienen gemeenten verantwoording af te leggen over de kwaliteit van de informatieveiligheid van diverse informatiesystemen met een nieuwe Audit systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG).

Kanttekeningen / alternatieven
Geen.

Financiële toelichting
Geen.

Juridische toelichting
Geen.

Publicatie
Geen.

Uitvoering

a. Planning
De rapportage informatieveiligheid en privacy zal voor 15 juli 2019 aan het ministerie van BZK worden gestuurd.

b. Communicatie

c. Evaluatie / controle
Verantwoording over informatieveiligheid middels ENSIA is een jaarlijks terugkerend proces.

Burgemeester en wethouders van Ooststellingwerf,

, secretaris , burgemeester.

A. Ter inzage liggende stukken

a. Rapportage informatieveiligheid en privacy 2018, Collegeverklaring ENSIA, Infographic ENSIA

B. Vertrouwelijke stukken

a.