ENSIA assurance rapport
DigiD en Suwinet
verantwoordingsjaar 2018
gemeente Gooise Meren

BKBO bv
Kenmerk BKBO/181019-4/AR
drs. M.B.H. IJpelaar RE CEH CISA

18 maart 2019
Dit assurancerapport heeft 10 pagina's
www.bkbo.nl

FEIT

Ook al zegt men dat
de wetenschap voor niets staat,
blijft het een feit
dat de zon voor niets opgaat.

Jules Deelder

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor

1.1 Ons oordeel

Wij hebben de bijgevoegde collegeverklaring ENSIA 2018 inzake informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van de gemeente Gooise Meren onderzocht.

Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van de gemeente Gooise Meren, in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

1.2 De basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de collegeverklaring verricht in overeenstemming met Richtlijn 3000-A (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance informatie voldoende en geschikt is als basis voor ons oordeel.

1.3 Beperking in gebruik en verspreidingskring

Dit assurancerapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Ons assurancerapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

1.4 Verantwoordelijkheden van het college van de gemeente Gooise Meren

Het college van burgemeester en wethouders van de gemeente Gooise Meren is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot Suwinet, zijn naast de collegeverklaring en dit assurance rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

- de risico's die het bereiken van de geselecteerde normen voor Suwinet in gevaar brengen, werden geïdentificeerd; en
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

Het College is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

1.5 Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de collegeverklaring nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de collegeverklaring en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang bevat;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van

inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen; en
- het evalueren van de toereikendheid van de assurance-informatie zoals opgenomen in de collegeverklaring en bijbehorende bijlage(n).

Vlijmen d.d. 18 maart 2019

Bureau voor Kwaliteitsborging Bij de Overheid b.v.


drs. M.B.H. IJpelaar RE CEH CISA, directeur

C.H.G. Schaap MA CISO, auditor in opleiding

Bijlage Rapport van bevindingen DigiD Mozard Suite

Deze bijlage is niet bestemd voor de verticale toezichthouder en wordt slechts verstrekt aan de gemeente Gooise Meren.

Bijlage Rapport van bevindingen DigiD iBurgerzaken

Deze bijlage is niet bestemd voor de verticale toezichthouder en wordt slechts verstrekt aan de gemeente Gooise Meren.

Bijlage Rapport van bevindingen Suwinet

Deze bijlage is niet bestemd voor de verticale toezichthouder en wordt slechts verstrekt aan de gemeente Gooise Meren.