At Risk Advies

College van B&W van gemeente Raalte
Postbus 140
8101 AC Raalte

Betreft: ENSIA rapportage gemeente Raalte
Datum: 5 april 2022
Kenmerk: 202203ERaalte

Assurance-rapport van de onafhankelijke IT-auditor
(Bij gebruik DigiD en Suwinet)

Aan: College van B&W van gemeente Raalte

Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2021 inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Raalte onderzocht.

Scope
De scope van ons onderzoek bestond uit de hierna genoemde Suwinet gegevensverwerkingen en DigiD aansluitingen:

Onderzochte gegevensverwerkingen Suwinet:

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	Binnen de gemeente en Uitkeringsadministratie en Sociale Recherche gemeente Deventer.	Nee / Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente en Uitkeringsadministratie en Sociale Recherche gemeente Deventer.	Nee /Ja

CONCEPT

Alleen voor identificatie doeleinden
M. Hommes RE

Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente en Uitkeringsadministratie en Sociale Recherche gemeente Deventer	Nee / Ja

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Niet van toepassing	Niet van toepassing
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Niet van toepassing	Niet van toepassing
Adresonderzoek door Burgerzaken	Niet van toepassing	Niet van toepassing

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam
1002569	Gemeente Raalte
1000313	Digitaal Loket Gemeente Raalte

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde DigiD aansluitingen en gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

Ons oordeel
Wij hebben de bijgevoegde collegeverklaring ENSIA 2021 inzake informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente Raalte onderzocht.

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

De collegeverklaring omvat het op 31 december 2021 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Wij benadrukken dat

Alleen voor identificatie doeleinden
M. Hommes RE

het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Benadrukking aangelegenheden

Zoals in de collegeverklaring is aangegeven wordt op 31 december 2021 niet aan alle normen inzake DigiD voldaan.

Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Een deel van deze verbeterplannen is na de peildatum, maar voor de rapportagedatum geëffectueerd.

Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

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.

Beperking in gebruik en verspreidingskring
Dit assurance-rapport 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 DigiD en Suwinet. Ons assurance-rapport 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.

Verantwoordelijkheden van het college van gemeente Raalte
Het college van burgemeester en wethouders van gemeente Raalte is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel

Alleen voor identificatie doeleinden
M. Hommes RE

CONCEPT

belang zijn in relatie tot DigiD en 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 DigiD en 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.

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:

CONCEPT

Alleen voor identificatie doeleinden
M. Hommes RE

- 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 bijlagen.

Maastricht, 5 april 2022

At Risk Advies BV

M. Hommes RE

CONCEPT

Alleen voor identificatie doeleinden
M. Hommes RE