Raadhuisplein 1
7811 AP Emmen
t. 14 0591
f. 0591 685599

Postbus 30001
7800 RA Emmen
e. gemeente@emmen.nl
i. gemeente.emmen.nl

Gemeente Emmen

Aan de raad van de gemeente Emmen

team
Informatie technologie

ons kenmerk	uw kenmerk	bijlage	behandeld door	BSN
18.021699		2	W. Stam	

datum	telefoon	fax	e-mail
5 september 2018	14 0591		gemeente@emmen.nl

onderwerp
Verantwoording informatiebeveiliging inzake DigiD, Suwinet, BAG en BGT in het kader van ENSIA

Geachte leden van de raad,

Op 31 december 2017 voldeden de interne beheersingsmaatregelen van de gemeente Emmen aan de normen inzake DigiD[1] en Suwinet[2]. Dit is door een externe auditor vastgesteld en met deze brief informeren wij u daarover.

Inleiding

Gemeenten hebben een belangrijke taak en verantwoordelijkheid in het op orde hebben en houden van informatiebeveiliging en het beschermen van (persoons)informatie. Steeds vaker krijgen gemeenten te maken met hacks, datalekken en beveiligingsincidenten. Informatieveiligheid en privacy hebben daarom een belangrijke plaats op de gemeentelijke agenda gekregen. Niet alleen het inrichten van adequate beveiligingsmaatregelen, maar ook het afleggen van verantwoording hierover is daarbij essentieel. Zo blijft informatieveiligheid en privacy van burgers gewaarborgd.

In de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente", vastgesteld tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de VNG op 29 november 2013, hebben gemeenten afgesproken zich elk jaar over de staat en de kwaliteit van hun informatieveiligheid te verantwoorden. Met ingang van het jaar 2017 gebeurt dit met een nieuwe auditsystematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). In de resolutie is ook vastgelegd dat wij verantwoording afleggen aan uw raad over de staat van de informatieveiligheid van de gemeente Emmen.

Verantwoordingsproces ENSIA

De focus van ENSIA ligt op het afleggen van horizontale verantwoording binnen de gemeente door een proces van zelfevaluatie. Deze verantwoordingssystematiek sluit aan op de gemeentelijke planning- en controlcyclus, waarmee de informatieveiligheid bestuurlijk en organisatorisch is geborgd. Dit is vastgelegd in het vastgestelde Informatiebeveiligingsbeleid Gemeente Emmen 2017-2020.

---

[1] Norm ICT-beveiligingsassessments DigiD versie 2.0
[2] Specifiek Suwinet normenkader Afnemers, versie 1.01 en bijlage 1 van de notitie

ENSIA structureert ook de verticale verantwoording richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI).

Samengevat kent het verantwoordingsproces van ENSIA de volgende stappen:

1. Uitvoeren zelfevaluatie gebaseerd op de BIG[3] en de geldende normenkaders voor BRP, PUN, DigiD en SUWI.
2. Opstellen rapportages en de collegeverklaring over SUWI en DigiD.
3. Uitvoeren van de IT-audit door een externe auditor.
4. Inleveren van de collegeverklaring en de assuranceverklaring van de externe auditor.

Collegeverklaring Informatiebeveiliging inzake DigiD en Suwinet
Op 30 april jl. hebben we door een 'Collegeverklaring' verantwoording afgelegd aan onze toezichthouders inzake DigiD en Suwinet. Voor Suwinet aan het ministerie van Sociale Zaken en Werkgelegenheid, voor DigiD aan Logius, onderdeel van het ministerie Binnenlandse Zaken en Koninkrijkrelaties (BZK). Hierin verklaren wij dat de gemeente Emmen voldoet aan de normenkaders voor DigiD en Suwinet. In het kader van de verantwoording DigiD zijn drie DigiD-aansluitingen getoetst aan het geldende normenkader.

De 'Collegeverklaring' is getoetst door een onafhankelijke, externe IT-auditor. Deze auditor heeft 'Assurance' gegeven op de Collegeverklaring. Dat wil zeggen dat op de toetsdatum 31 december 2017 onze interne beheersingsmaatregelen voldoen aan de normen inzake DigiD en Suwinet.

Verantwoordingsrapportage BAG en BGT
In het kader van ENSIA hebben we in 2017 ook een zelfevaluatie uitgevoerd voor de BAG en de BGT. Deze zelfevaluatie gaat in op vier kwaliteitscriteria: borging proces, volledigheid, tijdigheid en juistheid. De resultaten uit deze zelfevaluatie over het afgelopen jaar zijn niet auditplichtig en daarom niet gedeeld met de betreffende toezichthouders.

Verantwoording afleggen aan de raad
Met deze brief hebben wij u geïnformeerd over het verantwoordingsproces ENSIA.
Voor het afleggen van verantwoording wordt aangesloten bij de reguliere planning en controlcyclus.
In de jaarstukken wordt verantwoording afgelegd aan uw raad over de staat van de informatiebeveiliging.
Daarnaast wordt jaarlijks deze raadsbrief verstuurd.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
burgemeester en wethouders van Emmen,

de gemeentesecretaris,

I.A.A. Oostmeijer-Oosting

de burgemeester,

H.F. van Oosterhout

[3] Baseline Informatiebeveiliging Nederlandse Gemeenten

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Emmen legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigiD (aansluitnummers 999877 - Gemeente Emmen, 1001277 - Mijn SDV Gemeente Emmen, 1002009 - Belasting loket Emmen) en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA[3] voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring "bijlage 1 DigiD" blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD) en Suwinet (bijlage 2 Suwinet) geïnformeerd over de afwijkingen van de normen.

---

[1] https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/

[2] https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten

[3] https://www.ensia.nl/

ACCORIS

P.C.M. Holierhoek RERA

• 26 april 2018 •

voor indicatiedoeleinden

Gemeente Emmen

Verklaring college

Het college verklaart dat bij gemeente Emmen op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Emmen, 24 april 2018

Burgemeester en wethouders van Emmen

de gemeentesecretaris,

I.A.A. Oostmeijer-Oosting

de burgemeester, i.g.

H.F. van Oosterhout

ACCORIS
P.C.M. Holierhoek RERA
• 26 april 2018 •
voor indicatiedoeleinden

Assurancerapport van de onafhankelijke IT-auditor

Aan: College van burgemeester en wethouders van gemeente Emmen

Ons oordeel
Wij hebben de bijgevoegde Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de bijgaande Collegeverklaring wordt verwezen) van gemeente Emmen onderzocht.

Naar ons oordeel is bijgevoegde Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de Collegeverklaring wordt verwezen) van gemeente Emmen, in alle van materieel belang zijnde aspecten, juist.

De Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD en Suwinet (hierna Collegeverklaring ENSIA 2017) omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie verantwoordingsstelsel op website ENSIA voor de selectie van normen). Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel omtrent DigiD en Suwinet.

Benadrukking aangelegenheden
De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van de Collegeverklaring ENSIA 2017 en dit assurancerapport. Wij hebben wel vastgesteld dat onze assurance bij deze Collegeverklaring ENSIA 2017 en de assurance bij de verantwoording van de dienstverlener aan wie de beheersingsmaatregelen zijn uitbesteed tezamen de geselecteerde normen inzake DigiD afdekken.

In de collegeverklaring is vermeld dat op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord.

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 ENSIA 2017 uitgevoerd volgens Nederlands recht, waaronder de Richtlijn 3000 (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 ENSIA 2017'.

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.

ACCORIS
P.C.M. Holierhoek RERA
26 april 2018
'voor indicatiedoeleinden'

Beperking in gebruik en verspreidingskring
Dit assurancerapport is bestemd voor gebruikers van de Collegeverklaring ENSIA 2017. De Collegeverklaring ENSIA 2017 is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de Collegeverklaring ENSIA 2017 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 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.

Beperkingen van interne beheersingsmaatregelen
Interne beheersingsmaatregelen kunnen vanwege hun aard niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

Werking niet onderzocht
Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

Verantwoordelijkheden van het college van gemeente Emmen
Het college van burgemeester en wethouders van gemeente Emmen is verantwoordelijk voor het opstellen van de Collegeverklaring ENSIA 2017. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet dienen voldoende inzicht te hebben om deze Collegeverklaring ENSIA 2017, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang in relatie tot DigiD en Suwinet inschatten.

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 DigiD en Suwinet in gevaar brengen, werden geïdentificeerd;
- 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 ook verantwoordelijk is voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Collegeverklaring ENSIA 2017 mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Onze verantwoordelijkheden voor de assurance-opdracht betreffende de Collegeverklaring ENSIA 2017
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.

ACCORIS
P.C.M. Holierhoek RERA
• 26 april 2018 •
'voor indicatiedoeleinden'

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 ENSIA 2017 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 ENSIA 2017 en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen. Deze werkzaamheden hebben niet als doel om een oordeel uit te spreken over de effectiviteit van de interne beheersing van de gemeente;
- het op basis van deze kennis inschatten van de risico's dat de Collegeverklaring ENSIA 2017 onjuistheden van materieel belang bevat als gevolg van fraude en fouten, het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel. Bij fraude is het risico dat een afwijking van materieel belang niet ontdekt wordt groter dan bij fouten. Bij fraude kan sprake zijn van samenspanning, valsheid in geschrifte, het opzettelijk nalaten transacties vast te leggen, het opzettelijk verkeerd voorstellen van zaken of het doorbreken van de interne beheersing;
- 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.

Zoetermeer, 26 april 2018

Accoris Audit Services B.V.

P.C.M. Holierhoek RE RA
Managing Partner

ACCORIS
P.C.M. Holierhoek RERA
• 26 april 2018 •
'voor indicatiedoeleinden'