Aan:

College van Burgemeester en Wethouders
Gemeente Haarlem
d.t.v. de heer F. Hut, CISO
Zijlvest 39
2011 VB Haarlem
Verzonden per e-mail: fhut@haarlem.nl

Duijnborgh Audit b.v.

WTC Papendorp
Papendorpseweg 100
3528 BJ Utrecht
Postbus 40270
3504 AB Utrecht

T +31 (0)88 160 1700
F +31 (0)88 160 1799
I www.dbaudit.nl

IBAN: NL03 ABNA 0547 8300 25

KVK Midden Nederland
nr. 34224905

Plaats, datum	:	Utrecht, 3 juni 2020
Referentie	:	20200603 DBA GEM HLM her-audit Suwinet
Onderwerp	:	Aanvullende Assurance verklaring ENSIA 2019
Betreft	:	Gebruik Suwinet gegevens

Geacht college,

Ingevolge de opdracht van de gemeente Haarlem hebben wij een aanvullend onderzoek uitgevoerd met betrekking tot de opzet en het bestaan van specifieke maatregelen en procedures gericht op het gebruik van Suwinet gegevens door gemeente Haarlem. De aanleiding van dit onderzoek is dat tijdens de ENSIA audit 2019 enkele afwijkingen zijn vastgesteld met betrekking tot het gebruik van Suwinet gegevens.

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

Verantwoordelijkheden gemeente Haarlem

Gemeente Haarlem is verantwoordelijk voor het opzetten en implementeren van interne beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens.

Onze onafhankelijkheid en kwaliteitsbeheersing

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.

Duijnborgh Audit past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van oordelen over de opzet en bestaan van interne beheersingsmaatregelen per 3 juni 2020 voor het waarborgen van de vertrouwelijkheid van de Suwinet-gegevens die worden verwerkt door gemeente Haarlem. Wij hebben ons onderzoek verricht in overeenstemming met Nederlands recht, waaronder de Richtlijn 3000A, 'Assuranceopdrachten door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid.

Deze assurance-opdracht omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet en het bestaan van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de auditor van de organisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of niet bestaan. De werkzaamheden bestonden uit een combinatie van het kennisnemen van documentatie, het houden van interviews, het evalueren van de resultaten van de uitgevoerde interne controles en het verrichten van eigen (aanvullende) testwerkzaamheden.

Zoals hierboven staat vermeld, hebben wij geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen die bij de beschrijving waren inbegrepen en brengen derhalve daarover geen oordeel tot uitdrukking.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop een onderbouwing met een redelijke mate van zekerheid voor onze oordelen te bieden.

Gehanteerde criteria

Wij hebben bij de uitvoering van onze werkzaamheden gebruik gemaakt van de volgende normen en criteria (gezamenlijk verder aangeduid als normenkader):

- de Notitie Verantwoordingsstelsel ENSIA, versie 21 december 2017;
- de beveiligingsrichtlijnen uit het 'Specifiek Suwinet normenkader Afnemers, versie 1.01' dat is vastgesteld door het ketenoverleg van de Gezamenlijke elektronische Voorziening Suwinet (GeVS);
- bijlage 3 in de Handreiking ENSIA voor IT-auditors (RE's) van de NOREA, versie 2.0, 25 oktober 2018 (Guidance bij de te onderzoeken ENSIA-normen relevant voor Suwinet).

Wij achten deze criteria relevant en toereikend voor ons onderzoek.

Beperkingen

De 'ENSIA-normen voor Suwinet' zijn een selectie van beveiligingsrichtlijnen uit het 'Specifiek Suwinet normenkader Afnemers, versie 1.01' dat is vastgesteld door het ketenoverleg van de Gezamenlijke elektronische Voorziening Suwinet (GeVS). Daarom zijn we niet in staat om een overall oordeel te verschaffen omtrent de vertrouwelijkheid van de verwerking van Suwinet gegevens. Bovendien kunnen interne beheersingsmaatregelen bij een serviceorganisatie, vanwege hun aard, niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken. Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat kunnen worden of falen.

Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals ze zijn beschreven in deze rapportage. Per ENSIA-norm voor Suwinet wordt een oordeel gegeven over de opzet en het bestaan per 3 juni 2020. De criteria waarvan wij gebruik hebben gemaakt, zijn opgenomen in onderstaande tabel en een toelichting is te vinden in paragraaf 1.7.

Per beveiligingsrichtlijn hebben wij hieronder vermeld of met redelijke mate van zekerheid wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de conclusies in deze tabel weergegeven als “voldoet” of “voldoet niet”. Hierbij moet “voldoet” worden geïnterpreteerd als “Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm volgens de criteria genoemd in paragraaf 1.7 in alle materiële opzichten effectief zijn”. “Voldoet niet” moet worden geïnterpreteerd als “Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn volgens de criteria genoemd in paragraaf 1.7 niet in alle materiële opzichten effectief zijn”.

Suwinet Inkijk

Ref. Suwinet	Beveiligingsrichtlijn Suwinet	Referentie ENSIA vragenlijst	Oordeel ENSIA audit 2019	Oordeel her-audit 3 juni 2020
B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	▪ 5.1.1.A ▪ 5.1.1.B ▪ 6.1.1.A ▪ 6.1.2.A	Voldoet niet	Voldoet
B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	▪ 6.1.2.A	Voldoet	
B.05	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	▪ 6.1.3.A ▪ 10.1.3.B ▪ 10.1.3.C	Voldoet	
U.02	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.	▪ 11.2.1.A ▪ 11.2.1.B	Voldoet niet	Voldoet
U.03	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	▪ 11.2.1.A ▪ 11.2.1.B	Voldoet	
C.01	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën.	▪ 5.2.1.A ▪ 6.1.1.A	Voldoet niet	Voldoet

Ref. Suwinet	Beveiligingsrichtlijn Suwinet	Referentie ENSIA vragenlijst	Oordeel ENSIA audit 2019	Oordeel her-audit 3 juni 2020
C.04	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).	▪ 11.2.4.A	Voldoet deels, met aanbeveling	Voldoet
C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen).	▪ 10.10.2.A	Voldoet niet	Voldoet
AP[1]	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	▪ 8.2.2.A	Voldoet deels, met aanbeveling	Voldoet

Beoogde gebruikers en doel

Onze schriftelijke rapportage is alleen bestemd voor gemeente Haarlem, BKWI en het Ministerie van SZW en haar auditor(s), aangezien anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren. De rapportage, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming.

Voor zover het gemeente Haarlem is toegestaan het rapport aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Indien de producten van onze werkzaamheden aan derden ter beschikking worden gesteld, dient erop te worden gewezen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan het product kunnen worden ontleend. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

Utrecht, 3 juni 2020

Duijnborgh Audit B.V.

F. Kossen RE

(partner)

Drs. M. El Aarbaoui RE

(partner)

[1] Deze norm is toegevoegd naar aanleiding van de “Notitie verantwoordingsstelsel” van de Autoriteit Persoonsgegevens (AP).