

Gemeenteraad Rotterdam
Coolsingel 40
3011 AD Rotterdam

31 mei 2022

Betreft: Collegeverklaring ENSIA inclusief bijlagen DigiD en Suwinet

Geachte Raadsleden,

Op 19 april 2022 heeft u de Collegebrief inzake Collegeverklaring Gemeente Rotterdam ENSIA 2021 (kenmerk 22bb003280¹) ontvangen. Bij deze brief zat onder andere als bijlage de Collegeverklaring ENSIA 2021 inclusief de bijlagen DigiD en Suwinet. Bij het lezen van de collegebrief vielen mij een aantal feitelijke onjuistheden op. Daarnaast wordt in de collegebrief gesteld dat “het belang van openbaar maken van de informatie niet opweegt tegen het inzicht dat de inhoud van de bijlagen bieden in eventuele kwetsbaarheden in gebruikte systemen”. Deze stelling betwist ik. Graag ga ik onderstaand in op welke onjuistheden in de collegebrief staan en licht ik graag de redenen toe waarom de collegeverklaring ENSIA met haar bijlagen niet onder de geheimhouding valt. Aangezien de collegeverklaring nog niet inhoudelijk door uw raad is behandeld, heb ik ook nog enkele inhoudelijke vragen.

Feitelijke onjuistheden in de collegebrief

BIG vs BIO

Op pagina 2 wordt onder het kopje *Toelichting* gesteld dat het uitgangspunt voor de verantwoording de Baseline Informatiebeveiliging Gemeenten (BIG) is. Al sinds verantwoordingsjaar 2020 is de BIG vervangen door de Baseline Informatiebeveiliging Overheid (BIO). Overigens wordt (ook op pagina 2) onder de kop *Uitkomst audits op DigiD en Suwinet* wel weer geschreven over de BIO.

Vergelijkbaarheid door de jaren

Op pagina 2 wordt ook onder het kopje *Toelichting* het volgende gesteld: “Overigens wordt jaarlijks het normenkader voor de audits bepaald en/of aangepast. Dat betekent dat een vergelijking in tijd (bv. 2021 t.o.v. 2022) niet te maken is.” Alleen het eerste deel van deze stelling klopt, het tweede deel niet.

Voor DigiD is het normenkader (Norm ICT-beveiligingsassessments DigiD v2.0 van Logius) al sinds het begin van ENSIA in 2017 niet aangepast. Dat betekent dat juist voor DigiD de vergelijking door de tijd zeer goed te maken is. Overigens is het goed om hierbij op te merken dat van de 20 normen voor

¹ <https://gemeenteraad.rotterdam.nl/Agenda/Document/b8c8761c-abb9-424a-919a-72636309a284?documentId=3c17edcc-b18e-47c6-b1e2-c7fcf305a64e&agendatItemId=afd58b9c-7476-4cbf-9c7e-0575df284ee2>

DigiD er doorgaans 14 geheel zijn uitbesteed aan de leverancier van de applicatie waar de DigiD-aansluiting toegang toe geeft. Deze normen worden bij de leverancier door een IT-auditor getoetst. Middels een Third Party Memorandum (TPM) wordt door de leverancier aan de gemeente verantwoording afgelegd. Voor zes normen dient de gemeente zelf aanvullende beheersmaatregelen door te voeren om aan de normen te voldoen. Deze beheersmaatregelen binnen de gemeente hebben met name betrekking op het organisatorische/procesmatige vlak en nauwelijks op de ICT.

Voor Suwinet is in 2020 een nieuw normenkader opgesteld op basis van de BIO, namelijk Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2020 v1.0 van het BKWI. Voor 2021 kan dus zonder meer een vergelijking met 2020 gemaakt worden.

Voor onderbouwing van bovenstaande verwijs ik naar de ENSIA Notitie Verantwoordingsstelsel 2021², pagina 8 van de VNG. Hierin worden voor zowel DigiD als Suwinet geen wijzigingen in het normenkader aangekondigd.

Verzwarend normen

Op pagina 2 wordt ook onder het kopje *Uitkomst audits op DigiD en Suwinet* het volgende gesteld: “Vanuit de BIO zijn enkele normen voor DigiD en Suwinet voor dit jaar verzwakt, maar dit heeft geen impact gehad op de uiteindelijke eindscore.”

Zoals hierboven reeds gesteld zijn er voor zowel DigiD als Suwinet in 2021 geen wijzigingen en dus ook geen verzwakkingen in de normenkaders aangebracht.

Geheimhouding Collegeverklaring ENSIA 2021 inclusief de bijlagen DigiD en Suwinet Op basis waarvan geheim?

Het college verzoekt u geheimhouding op te leggen op basis van artikel 10, tweede lid, onder b, d en g, van de Wet Openbaarheid van Bestuur. De aanhef en subleden b, d en g van artikel 10, lid 2 van de WOB³ luidt als volgt:

Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:

- b. de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen;*
- d. inspectie, controle en toezicht door bestuursorganen;*
- g. het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.*

Wat staat er in de collegeverklaring en de bijlagen DigiD en Suwinet?

Om vast te stellen of de inhoud van de collegeverklaring ENSIA en haar bijlagen DigiD en Suwinet in

² <https://vng.nl/projecten/ensia>

³ https://wetten.overheid.nl/BWBR0005252/2018-07-28#HoofdstukV_Artikel10

strijd zijn met bovenstaande belangen, neem ik u allereerst graag mee door de inhoud van de collegeverklaring en de bijlagen DigiD en Suwinet.

De collegeverklaring ENSIA en de bijlagen DigiD en Suwinet zijn door de Vereniging van Nederlandse Gemeenten opgestelde standaard documenten. De enige inhoudelijke toevoegingen die de gemeente aan de verklaring doet is het opnemen van een tabel met DigiD en Suwinet-aansluitingen en aangeven of aan alle normen wordt voldaan. In de bijlage Suwinet wordt aangegeven voor welke taken Suwinet wordt gebruikt; of taken zijn uitbesteed en eventueel; aan welke normen niet wordt voldaan. Per DigiD-aansluiting wordt in de bijlagen DigiD een beknopte beschrijving gegeven van de DigiD-aansluiting; eventueel een verwijzing opgenomen naar een TPM; en wordt een overzicht opgenomen aan welke normen wel, of niet wordt voldaan.

Geen grond voor geheimhouding

Wanneer de collegeverklaring getoetst wordt aan de drie genoemde subleden van art 10, lid 2 van de WOB kan het volgende gesteld worden. Door het openbaar maken van welke DigiD- en Suwinet-aansluitingen de gemeente Rotterdam had in 2021 wordt geen economisch, of financieel belang van de gemeente Rotterdam (of een ander bestuursorgaan) geschaad. Ook of wel of niet aan alle normen (zonder te zeggen welke normen) wordt voldaan, schaadt geen enkel financieel of economisch belang.

Tevens schaadt het openbaar maken van de informatie uit de collegeverklaring niet de inspectie, controle en toezicht door uw raad. Het openbaar maken van die informatie zorgt wel voor grotere druk op het college en de uitvoeringsorganisatie(s) van de gemeente om aan alle normen uit de normenkaders te voldoen. Immers, slechte prestaties worden afgestraft.

Tot slot staan er in de collegeverklaring geen gegevens van natuurlijke, of rechtspersonen, waardoor ook dat deel van artikel 10, lid 2 geen grond geeft de collegeverklaring geheim te maken.

De gegevens in de bijlage DigiD met betrekking tot de DigiD-aansluitingen zijn van zo'n hoog abstract niveau dat deze nauwelijks gevoelig genoemd kunnen worden. De beschrijving van de aansluiting is zeer beknopt. Bovendien is deze informatie uit andere openbare bronnen ook te achterhalen. De voor het publiek meest interessante informatie uit de bijlage is of aan alle normen per DigiD-aansluiting niet wordt voldaan. Al deze gegevens schaden niet de belangen zoals genoemd in art. 10, lid 2 van de WOB.

Tot slot zijn de gegevens in de bijlage Suwinet tevens van een zeer abstract niveau. Hierin is bovendien geen sprake van een externe leverancier die een belang zou kunnen hebben. Uitsluitend de normen waar niet aan voldaan wordt, worden hier vermeld. Daarnaast hebben de normen uit het Suwinet-normenkader waar de gemeente verantwoording over aflegt geen betrekking op ICT-systemen, maar uitsluitend op organisatorische beheersmaatregelen. Er is in dit geval dus geen sprake van het openbaar maken van kwetsbaarheden in gebruikte systemen.

In zijn algemeenheid gaat ook het argument dat de informatie kwaadwillende in de kaart zou spelen hier niet op. Indien openbaar bekend wordt aan welke normen een DigiD- of Suwinet-aansluiting niet zou voldoen, levert dit geen bruikbare informatie op voor kwaadwillende. De normen met een

zeer technisch karakter zijn hoofdzakelijk belegd bij de leveranciers van de aansluitingen. De procedurele normen zijn hoofdzakelijk belegd bij de gemeente. Het grootste risico voor de gemeente is dat hackers gebruik maken van zwakheden in de technische infrastructuur van de aansluitingen. Echter, de formulering van de normen is niet zo specifiek dat daar een risico uit voortkomt. Immers, het niet voldoen aan de norm kan meerdere oorzaken hebben en hangt tevens samen met de technische infrastructuur van de aansluiting.

Tot slot, weegt ook het openbaar belang van de informatie uit de collegeverklaring en haar bijlagen zwaar. Immers, middels de Suwinet-aansluiting(en) van de gemeente Rotterdam zijn van alle Rotterdammers zeer veel privacy gevoelige gegevens in te zien. Juist in Rotterdam is het in het verleden op dit gebied mis gegaan^{4 5}.

Via DigiD loggen veel Rotterdammers dagelijks in op de gemeentelijke website om een uiteenlopende zaken te regelen. Dat kan gaan om het verlengen van een parkeervergunning, maar ook om het aanvragen van een uitkering. Voor zowel DigiD als Suwinet is het voor de Rotterdammers dus van belang dat deze aansluitingen goed, maar vooral veilig werken. Publiekelijk verantwoording afleggen over de veiligheid van deze aansluitingen is het sluitstuk van de controle op die veiligheid.

Gezien bovenstaande overwegingen weegt het openbaar belang van deze informatie zwaarder dan de belangen van de gemeente. Om die reden verzoek ik u tegen de geheimhouding van de collegeverklaring ENSIA en de bijlagen DigiD en Suwinet te stemmen.

Vragen Collegeverklaring ENSIA 2021 inclusief de bijlagen DigiD en Suwinet

Aangezien de collegeverklaring ENSIA (nog) niet openbaar is voor het publiek, maar wel voor u, is het moeilijk daar voor mij inhoudelijke vragen over te stellen. Toch zou ik u graag de volgende vragen en overpeinzingen willen mee geven.

DigiD

1. Aangezien het normenkader voor DigiD sinds het begin van ENSIA (2017) niet is aangepast, zou bij een bestaande DigiD-aansluiting het beheersproces rondom de aansluiting al jaren min of meer hetzelfde moeten zijn. Indien bij zo'n aansluiting vorig jaar aan alle normen werd voldaan, en dit jaar niet, is dat een signaal dat er binnen de gemeente dus iets moet zijn verandert waardoor de gemeente slechter is gaan presteren. Dat roept de vraag op: wat heeft er voor gezorgd dat de gemeente slechter is gaan presteren?
2. Als vorig jaar bij een aansluiting aan een norm niet werd voldaan en dit jaar ook niet, dan heeft het verbeterplan van vorig jaar (wat verplicht wordt opgesteld na het niet voldoen aan een norm) gefaald. Wat is hier dan de reactie van Logius (beheersorganisatie DigiD) op

⁴ <https://www.vpro.nl/argos/media/afleveringen/2015/Lek-Suwinet.html>

⁵ <https://decorrespondent.nl/1703/als-stagiair-opzoeken-wat-de-baas-verdient-bij-de-gemeente-kan-het/156180879998-080defbf>

geweest? Hoe wordt gezorgd dat het verbeterplan dit jaar wel voldoet?

3. Indien er in 2021 nieuwe DigiD-aansluitingen zijn gerealiseerd door de gemeente, worden deze nog niet in de collegeverklaring ENSIA over 2021 meegenomen. Binnen twee maanden na het openen van een nieuwe DigiD-aansluiting door Logius, dient de gemeente voor die aansluiting een aparte IT-audit te laten uitvoeren. Zijn er in 2021 nieuwe DigiD-aansluitingen door de gemeente Rotterdam geopend? Wat waren de uitkomsten van de IT-audit(s) voor die aansluiting(en)?

Suwinet

4. Zoals reeds eerder in deze brief vermeld is het normenkader voor Suwinet in 2020 grondig aangepast. Hoewel de beheersomgeving nog steeds aan minimaal dezelfde eisen moet voldoen is de opzet van het normenkader aangepast. Voor 2021 zijn er geen wijzigingen ten opzichte van 2020. Indien bij de Suwinet-aansluiting(en) vorig jaar aan alle normen werd voldaan, en dit jaar niet, is dat een signaal dat er binnen de gemeente dus iets moet zijn veranderd waardoor de gemeente slechter is gaan presteren. Wat heeft er voor gezorgd dat de gemeente slechter is gaan presteren?

Ik hoop u met deze brief meer inzicht in ENSIA te hebben gegeven en handvatten voor uw controlerende taak. Ik wens u veel succes en sterkte toe.

Met vriendelijke groet,