



**Gemeente
Rotterdam**

Bestuurs- en Concernondersteuning
Financiën en Organisatie, Dienstverlening, Grote
Projecten
Maarten Struijvenberg

Postadres: Postbus 70012
3000 KP Rotterdam
Website: www.rotterdam.nl

Van: Özgür Dogan
Telefoon: 14 010
E-mail: bbo@rotterdam.nl

Ons kenmerk: M2303-3010 - 23bo4305

Onderwerp: Collegeverklaring ENSIA

Datum: B&W 11 april 2023

Aan de gemeenteraad

Onderwerp:

Onder oplegging van geheimhouding inzicht geven in de collegeverklaring ENSIA

Op welke gronden deze brief?/Waarom nu voorgelegd?

Hierbij wordt het volgende document gedeeltelijk onder geheimhouding aan u voorgelegd: Collegeverklaring ENSIA.

Met de voorliggende brief informeren wij u over de ENSIA-resultaten van het verantwoordingsjaar 2022. Per 1 juli 2017 verantwoordten gemeenten in Nederland zich over informatiebeveiliging conform de Eenduidige Normatiek Single Information Audit (ENSIA). Middels een grootschalige zelfevaluatie beoordelen gemeenten de mate waarin ze aan informatiebeveiliging voldoen op basis van enkele normenkaders/wetgeving, waarvan het grootste normenkader de Baseline Informatiebeveiliging Overheid (BIO) betreft.

Het doel van de ENSIA is om gemeentelijke organisaties op een eenduidige en transparante manier richting de gemeenteraad -de horizontale verantwoording- en richting het Rijk -de verticale verantwoording- verantwoording af te laten leggen over de mate waarin deze in control zijn op het vlak van de informatiebeveiliging van verscheidene aansluitingen en landelijke systemen, zoals de basisregistraties, Suwinet en DigiD.

Conform de landelijke richtlijnen moet de uitkomst van ENSIA uiterlijk 15 juli worden gedeeld met de gemeenteraad, inclusief een overzicht met de eventueel benodigde verbetermaatregelen ('verbeterplannen'). Met het toezenden van de voorliggende brief geeft ons college hier invulling aan.



Geheimhouding

Wij verstrekken u “ de Collegeverklaring over de audits op de DigiD en Suwinet aansluitingen” gedeeltelijk onder oplegging van geheimhouding krachtens de artikelen 87 en 88, tweede lid, van de Gemeentewet jo. artikel 5.1, tweede lid, sub e, h en i van de Wet open overheid. De geheimhouding rust op de gelakte/gearceerde delen. Een ongelakte versie treft u aan in de digitale kluis.

Het belang van het openbaar maken van deze informatie weegt niet op tegen het risico van oneigenlijke toegang tot de data van de gemeente Rotterdam en het bieden van inzicht in eventuele kwetsbaarheden.

Wij stellen op grond van ons beleidskader ‘verstrekking openbare en geheime informatie aan de raad’ voor na één jaar (11 april 2024) een herbeoordeling te doen van de geheimhouding.

Relatie met het coalitieakkoord/collegewerkprogramma/eerder aangenomen moties en gedane toezeggingen:

N.v.t

Toelichting:

De gemeenteraad van Rotterdam wordt op verschillende wijzen periodiek geïnformeerd over de stand van zaken rondom informatiebeveiliging. Enerzijds wordt de gemeenteraad jaarlijks via de reguliere P&C cyclus geïnformeerd over het informatiebeleid, inclusief het informatiebeveiligingsbeleid. Aanvullend wordt de gemeenteraad, zoals beschreven, jaarlijks op de hoogte gebracht van de mate waarin de gemeente Rotterdam in control is op het gebied van informatiebeveiliging middels de ENSIA-systematiek. ENSIA voorziet door middel van het uitvoeren van een zelfevaluatie in verantwoording op het gebied van de volgende kaders/wetten:

- Baseline Informatiebeveiliging Overheid (BIO)
- Basisregistratie Personen (BRP)
- Wet- en regelgeving Reisdocumenten (PUN en PNIK)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Gemeenschappelijke elektronische Voorziening Suwi (Suwinet)
- Waardering Onroerende Zaken (WOZ)

Het doel van ENSIA is om in één systematiek de verantwoording over deze koppelingen te bundelen en daarmee in één keer verantwoording af te leggen over de toepassing van deze stelsels.

Aanvullend op deze zelfevaluatie vindt er op Suwinet en DigiD jaarlijks een onafhankelijke externe IT-audit plaats.



Deze externe IT-audit vindt plaats op de collegeverklaring ENSIA waarin het college van B&W verklaart aan welke Suwinet en DigiD normen op 31 december 2022 wel of niet werd voldaan op het gebied van de opzet en het bestaan van de beheersingsmaatregelen. Indien de externe IT-auditor vaststelt dat de collegeverklaring een getrouw beeld geeft van de werkelijkheid, dan geeft deze hier een goedkeurende verklaring over af in de vorm van een assurance rapportage. Binnen de gemeente Rotterdam is deze audit uitgevoerd door Concernauditing.

In de bijlage vindt u ter informatie de Collegeverklaring over de audits op de DigiD en Suwinet aansluitingen. Dit document bevat geheime passages. Daarnaast treft u ook de verantwoordingsrapportages BAG, BGT, BRO en WOZ. De verantwoording over de Basisregistratie Personen en Wet- en regelgeving Reisdocumenten verloopt middels een eigen proces en valt om deze reden buiten dit verantwoordingsmoment.

Uitkomst audits op DigiD en Suwinet

Ten opzichte van vorig jaar kan geconcludeerd worden dat er significante verbeteringen hebben plaatsgevonden ten aanzien van de vastlegging van beveiligingsactiviteiten op alle niveaus van de organisatie. Tegelijk geldt dat er een aanscherping heeft plaatsgevonden in de auditmethodologie waardoor er op sommige vlakken dieper is ingezoomd op specifieke onderwerpen. Hoewel Rotterdam de meeste beheersingsmaatregelen op een juiste wijze heeft doorgevoerd, geldt dan ook dat een enkel onderwerp nog nadere uitwerking behoeft, waardoor in de collegeverklaring niet kon worden aangegeven aan alle getoetste normen te voldoen.

Op 31 december 2022 werd niet voldaan aan zes DigiD normen. Vijf van de zes normen vloeien in elkaar over daar deze dezelfde technische implementatie kennen. Het merendeel van deze beperkingen is inmiddels opgelost. Echter, aangezien opnieuw onafhankelijk vastgesteld dient te worden dat deze risico's zijn gemitigeerd, kan nog niet formeel worden verklaard dat deze bevindingen zijn verholpen. Voor de laatste norm die nog niet voldoet, geldt dat er onvoldoende is vastgelegd dat rechten van een specifieke groep beheerders periodiek worden gecontroleerd.

Voor Suwinet is één tekortkoming geconstateerd. Hiervoor geldt dat er een aanscherping dient te worden uitgevoerd op de controles van de logbestanden van een specifieke applicatie.

Voor de normen van DigiD en Suwinet waar bevindingen voor zijn, zijn verbeterplannen opgesteld. Naar verwachting zullen de verbeteringen voor DigiD vòòr 1 juli 2023 zijn doorgevoerd en in het geval van Suwinet voor het einde van het jaar. In de bijlage treft u de collegeverklaring met het bijbehorende overzicht van normen waaraan wel en niet is voldaan per 31 december 2022.

Uitkomst meting BAG, BGT, BRO en WOZ

Hoewel er specifiek over Suwinet en DigiD een onafhankelijke audit plaatsvindt, vindt er tevens verticale verantwoording plaats over de basisregistratie voor Adressen en Gebouwen (BAG), Grootchalige Topografie (BGT) en Registratie Ondergrond (BRO). Daarnaast dienen gemeenten zich sinds 2021 aanvullend te verantwoorden over de mate waarin de beveiligingsmaatregelen voor de WOZ zijn doorgevoerd.

De uitkomsten van deze zelfevaluaties zijn opgenomen in de rapportages die als bijlage bij deze brief zijn gevoegd. Bij de BGT is een score van 100% gehaald (100% in 2021), bij de BAG 72% (83% in 2021) en bij de BRO 88% (77% in 2021).



Deze scores hebben betrekking op de juridische verankering, de actualisatie van procesbeschrijvingen, herijking van formatie en het wegwerken van achterstanden. Zoals te zien aan de scores ten opzichte van vorig jaar, zijn er verbeteringen doorgevoerd op de BRO, heeft de BGT wederom de maximale score weten te behouden en laat de BAG een lichte daling in de score zien. Deze daling wordt veroorzaakt door personele tekorten waardoor er achterstanden zijn ontstaan in de verwerking van meldingen. Inmiddels is een kwaliteitsmedewerker gestart welke bijdraagt aan het inlopen van de opgelopen achterstanden.

Voor de WOZ geldt dat er in 2022 aan een drietal normen niet is voldaan. De reden voor deze non-compliance is goed verklaarbaar. Zo worden er nog geen controles uitgevoerd op BIO ontwikkelingen daar de WOZ zich in het voortraject van de BIO implementatie bevindt.

Verbeterplannen

Zoals aangegeven is in 2022 niet aan alle normen voor Suwinet en DigiD voldaan. Om deze reden zijn er verbeterplannen opgesteld waarin staat beschreven welke acties dienen te worden uitgevoerd om alsnog aan de betreffende normen te voldoen. Wij zijn in staat om de bevindingen binnen de daarin gestelde termijn van 1 juli te hebben opgelost. Desgewenst kan een toelichting worden gegeven op de inhoud van de verbeterplannen. Tot slot benadrukt het college dat het belang van een juiste beveiliging van informatie goed wordt ingezien en de nodige middelen worden ingezet om de ontbrekende beveiligingsmaatregelen zo snel mogelijk door te voeren.

Financiële en juridische consequenties/aspecten:

N.v.t.

Burgemeester en Wethouders van Rotterdam,

De secretaris,	De burgemeester,
V.J.M. Roozen	A. Aboutaleb

Bijlage(n):

Bijlage 1: Gelakte collegeverklaring ENSIA (inclusief bijlagen DigiD en Suwinet) (GEDEELTELIJK GEHEIM) **ten behoeve van publicatie.**

Bijlage 2: Ongelakte collegeverklaring ENSIA (inclusief bijlagen DigiD en Suwinet) **ten behoeve van de digitale kluis.** (GEDEELTELIJK GEHEIM)

Bijlage 3: Verantwoordingsrapportage BAG, BGT en BRO

Bijlage 4: Verantwoordingsrapportage WOZ