

Aan: Gemeenteraad Rotterdam
Coolsingel 40
3011 AD Rotterdam

8 juni 2022

Betreft: Collegeverklaring ENSIA inclusief bijlagen DigiD en Suwinet

Geachte Raadsleden,

Naar aanleiding van het openbaar worden van de collegeverklaring ENSIA en de bijlagen DigiD en Suwinet stuur ik u in navolging van mijn brief van 31 mei jongstleden bijgaand mijn aanvullende vragen.

Suwinet

Uit de bijlage Suwinet blijkt dat er op 31 december 2021 aan vier normen niet werd voldaan, maar op 1 februari 2022 wel.

1. Heeft er in 2021 een interim controle plaatsgevonden door de auditor ten aanzien van Suwinet?
 - a. Zo nee, waarom niet? Op basis van deze controle hadden de bevindingen vroegtijdig gesignaleerd kunnen worden en hadden deze voor 31 december kunnen worden geadresseerd.
 - b. Zo ja, waarom zijn de geconstateerde bevindingen niet voor 31 december geadresseerd?
2. Heeft de auditor na 31 december 2021 vastgesteld dat de gemeente Rotterdam aan alle Suwinet-normen voldeed?

De collegeverklaring heeft alleen betrekking op de opzet en het bestaan van de beheersmaatregelen in het normenkader. Hierbij is dus nog niet eens de werking van deze beheersmaatregelen betrokken. (Immers, dit ligt buiten de scope van ENSIA.) Indien aan een norm niet wordt voldaan is dus of de opzet van de beheersmaatregel onvoldoende en/of het bestaan kan niet worden vastgesteld. Dit laatste betekent dat de beheersmaatregel in 2021 dus niet zou zijn uitgevoerd.

3.
 - a. De toegangsrechten van Suwinet-gebruikers dienen volgens norm 9.2.5.3 minimaal twee keer per jaar beoordeeld te worden. Hiermee wordt voorkomen dat deze rechten als gevolg van bijvoorbeeld een wijziging in taken van een ambtenaar te ruim worden. Hoe vaak zijn de toegangsrechten van Suwinet-gebruikers binnen de gemeente Rotterdam in 2021 gecontroleerd?
 - b. Zijn naar aanleiding van die controle (indien nodig) toegangsrechten van gebruikers gewijzigd?

4. Norm 12.4.1 stelt dat de logging van het gebruik van Suwinet door gebruikers periodiek moet worden beoordeeld met als doel onrechtmatig gebruik van Suwinet op te sporen. Aan deze norm wordt door de gemeente Rotterdam niet voldaan.
 - a. Indien de logging in 2021 niet is beoordeeld, is dit dan achteraf alsnog gedaan?
 - b. Is uit de beoordeling van de logging onrechtmatig gebruik gebleken?

DigiD

5. Is door de auditor geconstateerd of per heden bij alle DigiD-aansluitingen wel aan het normenkader wordt voldaan?

Aansluiting Mijn Loket – 1000161

Uit de collegeverklaring blijkt dat de DigiD-aansluiting *Mijn Loket* geheel maatwerk is en wordt onderhouden door de gemeente zelf. Tevens wordt bij deze aansluiting door de gemeente (dus niet bij de ICT-leverancier) aan vijf normen niet voldaan. Bij de andere drie aansluitingen gaat het om standaard applicaties van een leverancier. Hier wordt door de gemeente wel aan alle normen voldaan. Dit toont aan dat het risico bij een maatwerk applicatie, die notabene door de gemeente zelf wordt onderhouden, groter is dan bij een standaard applicatie van een leverancier.

6. Heeft er in 2021 een interim controle plaatsgevonden door de auditor ten aanzien van deze DigiD-aansluiting?
 - a. Zo nee, waarom niet? Op basis van deze controle hadden de bevindingen vroegtijdig gesignaleerd kunnen worden en hadden deze voor 31 december kunnen worden geadresseerd.
 - b. Zo ja, waarom zijn de geconstateerde bevindingen niet voor 31 december geadresseerd?
7. Vindt de gemeente dat het risico van een maatwerk applicatie waard is in vergelijking met die van een standaard applicatie en wat maakt dit grotere risico acceptabel/nodig?

Ik hoop u met deze vragen geholpen te hebben met uw controlerende taak. Ik wens u veel succes en sterkte toe.

Met vriendelijke groet,