Gemeente Diemen

2e kwartaalbrief 2022

Versie: Vastgesteld door Raad

14 juli 2022

2.2 Voortgang toegezegde onderwerpen Raad

In deze paragraaf wordt de Raad geïnformeerd over de voortgang van toegezegde onderwerpen. Het is niet nodig dat de Raad hierover een besluit neemt.

2.2.1 Informatieveiligheid

Programma Samen Besturen

Wanneer nodig wordt de raad in de kwartaalbrief geïnformeerd over ontwikkelingen op het gebied van informatieveiligheid. In deze kwartaalbrief wordt een terugkoppeling gedaan over de auditresultaten 2021.

Instemming college met nieuw normenkader, de Baseline voor Overheidsinstellingen (BIO)
Al eerder kondigden we aan dat per 1 januari 2020 jl. de huidige
Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), het normenkader voor informatieveiligheid, is overgegaan naar een nieuwe gezamenlijke Baseline voor Overheidsinstellingen, de BIO. De achterliggende reden is om de informatiebeveiliging verder optimaal te professionaliseren voor de gehele overheid. De BIO is gebaseerd op de internationaal erkende en actuele ISO-normatiek. Het uiteindelijke doel hiervan is te komen tot een veilige digitale overheid.

Als gevolg van dit nieuwe normenkader heeft het college begin december 2020 ook het bestaande Strategisch Informatieveiligheidbeleid aangepast aan deze nieuwe normering.

Instemming andere DUO-gemeenten en bestuur Uitvoeringsorganisatie Duo+
Ook de andere DUO-gemeenten en het bestuur van de Duo+ uitvoeringsorganisatie hebben ingestemd met de wijziging van het normenkader, de BIO. Dit betekend dat alle DUO-organisaties tezamen dit beleid ondersteunen.

Welke gevolgen heeft dit?
De verandering van het normenkader betekent dat er een aanpassing van het gehele informatieveiligheidbeleid moet worden doorgevoerd.

De BIO legt meer nadruk op het risicomanagement en stelt strengere eisen aan het nemen van specifieke maatregelen. De rol van de bestuurder en lijnmanager(s) is ook ten aanzien van risicomanagement explicieter dan voorheen.

Daarnaast is ook de jaarlijkse ENSIA (Eenduidige Normatiek Single Information Audit) cyclus, met ingang van het verantwoordingsjaar over 2020, gebaseerd op de nieuwe BIO-normering.

Toelichting

Het informatieveiligheid betreft drie onderwerpen, te weten:
1. de Baseline Informatieveiligheid Overheid (BIO);
2. de Eenduidige Normatiek Single Information Audit (ENSIA) - jaarlijkse verantwoording aan de toezichthouders vanuit het Rijk;
3. de Algemene verordening gegevensbescherming (AVG 2018) - wettelijke verplichting.

Eenduidige Normatiek Single Information Audit (ENSIA)
ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatie-veiligheid. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale Identiteit (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

De afzonderlijke, zogenoemde verticale verantwoording, geschied aan landelijke partijen en ministeries die een rol hebben in het toezicht op informatieveiligheid. De afzonderlijke verantwoordingen zijn de basis voor de, zogenoemde horizontale verantwoording, aan de gemeenteraad. Net als in eerdere jaren moest ook deze zelfevaluatie vóór 31 december 2020 worden aangeleverd. Dit is voor alle DUO-gemeenten op tijd gelukt.

Onderdeel van het verantwoordingsproces ENSIA is het afgeven van een Collegeverklaring per gemeente. Deze zogenoemde ‘Collegeverklaring’ betreft over 2020 het gebruik van DigiD en Suwinet. Besluitvorming hieromtrent valt onder de verantwoordelijkheid van het college van burgemeester en wethouders. Het college is verplicht de raad te informeren, de wijze waarop is vormvrij.

Resultaat ENSIA audit 2020
De jaarlijkse ENSIA Cyclus heeft in 2020 voor het derde jaar in de vorm van een zelfevaluatie plaatsgevonden. Diemen en de andere DUO-gemeenten doen dit goed ten opzichte van andere gemeenten. Er is wederom veel werk verricht om de verantwoording tijdig aan te leveren. Ten opzichte van de resultaten over 2019 heeft er een verdere verbetering plaats gevonden welke heeft geleid tot het "voldoen" aan alle gestelde voorwaarden.

Het toetsingskader voor de ENSIA-audit bestaat uit maatregelen op het gebied van Beleid, Uitvoering en Controle. In de uitgevoerde zelfevaluatie en de daarop volgende IT-audit naar aanleiding van de bevindingen is gebleken dat er op operationeel niveau in voldoende mate afspraken zijn gemaakt, die een volledig voldoen aan gestelde kwaliteitsnormen informatieveiligheid rechtvaardigen.