

2e kwartaalbrief 2024

Versie: Vastgesteld door Raad

18 Juli 2024



2.2.2 Informatieveiligheid

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 2023.

Baseline voor Overheidsinstellingen (BIO)

Voor overheidsinstellingen geldt sinds 2020 de Baseline Informatieveiligheid Overheid, de BIO. De achterliggende reden is om de informatiebeveiliging verder optimaal te professionaliseren. De BIO is gebaseerd op de internationaal erkende en actuele ISO-normatiek en draagt bij aan een professionalisering van Informatiebeveiliging met als doel een veilige digitale overheid. Als gevolg van dit normenkader heeft het college begin december 2020 ook het bestaande Strategisch informatieveiligheidsbeleid aangepast aan deze nieuwe normering.

De BIO legt nadruk op het risicomanagement en stelt strengere eisen aan het nemen van specifieke maatregelen. Ook de rol van de bestuurder en lijnmanager(s) inzake het veilig houden van Informatie kent eigen verantwoordelijkheden. De jaarlijkse ENSIA (Eenduidige Normatiek Single Information Audit) cyclus is ook gebaseerd op de BIO-normering.

Toelichting Informatieveiligheid betreft vier 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.
4. de Wet politiegegevens (Wpg).

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

De afzonderlijke, zogenoemde verticale verantwoording, geschiedt 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 2023 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 2023 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 2023

De jaarlijkse ENSIA Cyclus heeft in 2023 opnieuw in de vorm van een zelfevaluatie plaatsgevonden gevolgd door nader onderzoek door een externe audit partij op de specifieke onderdelen van de BIO voor Suwinet en DigiD. 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 2022 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 uitgebreide IT-audit naar aanleiding van de bevindingen is gebleken dat er ook voor de bevindingen op operationeel niveau in 2023 in voldoende mate afspraken zijn gemaakt, die volledig voldoen aan gestelde kwaliteitsnormen.