Gemeente Almelo

Raadsbrief ter informatie

Postadres:
Gemeente Almelo
Postbus 5100
7600 GC Almelo

Aan de raad van de gemeente Almelo

Doorkiesnummer	Behandeld door	Datum
541765	A. de Boer	6 april 2021

Onderwerp
Auditresultaten ENSIA rapportage informatiebeveiliging 2020

Geachte raadsleden,

Gemeenten hebben een belangrijke taak en verantwoordelijkheid als het gaat om het op orde hebben van informatiebeveiliging en het beschermen van informatie. Steeds vaker worden gemeenten geconfronteerd met hacks, datalekken en beveiligingsincidenten. Informatieveiligheid en privacy hebben daarom een belangrijke plaats op de gemeentelijke agenda. Het adequaat inrichten van verantwoordingsprocessen is daarbij essentieel. Zo blijft informatieveiligheid en privacy van burgers gewaarborgd.

In deze brief informeren wij u over de ENSIA auditresultaten. ENSIA staat voor Eenduidige Normatiek Single Information Audit en is een jaarlijks verplichte verantwoordingsrapportage. De gemeente Almelo voldoet aan de gestelde eisen en normen voor DigiD en Suwinet en voor de drie geo-basisregistraties scoren we een voldoende en voldoen we zodoende aan de gestelde eisen en normen. Hieronder lichten we het verder toe.

ENSIA systematiek

Gemeenten dienen zich elk jaar te verantwoorden over de status van de informatieveiligheid van diverse informatiesystemen. Met ingang van 2017 is er een nieuwe systematiek voor verantwoording van de informatiebeveiliging ingevoerd, de ENSIA systematiek. Deze systematiek vloeit voort uit een resolutie van de Buitengewone Algemene Ledenvergadering van de VNG.

Met ENSIA wordt het verantwoordingsproces rondom informatieveiligheid gestroomlijnd. ENSIA neemt met ingang van 2020 het nieuwe normenkader voor de gehele overheid de BIO (Baseline Informatiebeveiliging Overheid) als uitgangspunt en de zelfevaluatie bestaat uit enkele honderden vragen. Vanuit deze horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij het rijk afgeleid, de zogenaamde verticale verantwoording.

Diverse informatiesystemen en verantwoording

Met ENSIA is er één verantwoordingsprocedure voor de Basisregistratie Personen (BRP), de Paspoortuitvoeringsregeling (PUN), de Digitale persoonsidentificatie (DigiD), de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Dit betekent dat er niet voor alle onderdelen afzonderlijke audits (die elkaar deels overlappen) moeten worden uitgevoerd. Er hoeven dan ook geen afzonderlijke rapportages opgesteld te worden. In al deze registratiesystemen wordt belangrijke informatie verwerkt en moeten we maatregelen nemen om de informatie veilig te houden.

Collegeverklaring informatiebeveiliging inzake DigiD en Suwinet

Voor 1 mei 2021 dienen we verantwoording af te leggen richting onze verticale toezichthouders inzake DigiD en Suwinet. Voor Suwinet aan het ministerie van Sociale Zaken en Werkgelegenheid, voor DigiD aan Logius, onderdeel van het ministerie Binnenlandse Zaken en Koninkrijkrelaties (BZK).

Voor Suwinet en DigiD is op basis van de zelfevaluatie binnen ENSIA en de normenkaders die gelden voor DigiD en Suwinet een collegeverklaring opgesteld. Hierin verklaart het college dat de gemeente Almelo voldoet aan de geldende eisen en normen inzake DigiD en Suwinet.
Voor DigiD zijn er twee webapplicaties waarvoor wij een DigiD-aansluiting hebben onderzocht.

De collegeverklaring is getoetst door een onafhankelijke, externe IT-auditor. Deze auditor heeft assurance gegeven op de collegeverklaring. Op basis van de collegeverklaring en onderliggende documenten en verklaringen hebben wij ons verantwoord richting de verticale toezichthouder en tonen we aan dat we voldoen aan de gestelde normen voor DigiD en Suwinet. Hiermee wordt het gebruik van Suwinet en de DigiD-aansluiting ook in de toekomst geborgd.
De externe IT-auditor heeft op grond van de gedane bevindingen geen tekortkomingen geconstateerd en daarmee geen verbeterpunten aangegeven. Wel heeft de auditor naast het assurancerapport voor intern gebruik rapporten van bevindingen opgesteld. In deze documenten zijn enkele aanbevelingen opgenomen om de kwaliteit van informatiebeveiliging nog verder te verbeteren.

Verantwoordingsrapportage BAG, BGT en BRO

In het kader van ENSIA hebben we in 2020 ook een zelfevaluatie uitgevoerd voor de BAG, BGT en de BRO. Deze zelfevaluatie gaat in op vier kwaliteitscriteria: borging proces, actualiteit, volledigheid en juistheid. De resultaten uit deze zelfevaluatie moeten voor 1 mei gedeeld zijn met de toezichthouder (het ministerie van BZK) met verantwoordingsrapportages voor de BAG, BGT en BRO. Voor deze basisregistraties scoren we een voldoende, boven de normscore, en voldoen zodoende aan de gestelde eisen en normen en lopen we geen risico's. De rapportages leveren wel enkele verbeterpunten op.

Verantwoording afleggen aan de raad

Voor het afleggen van verantwoording aan de gemeenteraad wordt er aangesloten bij de planning en control cyclus van de gemeente. In het jaarverantwoording wordt er verantwoording afgelegd over informatiebeveiliging aan de gemeenteraad.

Op grond van artikel 25, tweede lid van de Gemeentewet, hebben we geheimhouding opgelegd op de collegeverklaring, bijlage 1 DigiD en bijlage 2 Suwinet van de collegeverklaring en het assurancerapport van de IT auditor. Deze stukken zijn op aanvraag in te zien bij de griffie.

Hoogachtend,

Burgemeester en Wethouders van Almelo,
de secretaris, de burgemeester,

F.W. van Ardenne A.J. Gerritsen