

Raadsbrief ter informatie

Postadres:
Gemeente Almelo
Postbus 5100
7600 GC Almelo

Aan de raad van de gemeente Almelo

Doorkiesnummer
541765

Behandeld door
A. de Boer

Datum
23 april 2019

Onderwerp
Auditresultaten ENSIA rapportage informatiebeveiliging

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.

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 en dit staat voor Eenduidige Normatiek Single Information Audit. Deze systematiek vloeit voort uit een resolutie van de Buitengewone Algemene Ledenvergadering van de VNG.

Met ENSIA wordt het verantwoordingsproces rondom informatieveiligheid gestroomlijnd en kunnen wij zowel verticaal, aan de ministeries, als horizontaal verantwoording afleggen aan de gemeenteraad. ENSIA neemt de Baseline Informatiebeveiliging Gemeenten (BIG) 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. Voor de uitvoering wordt gebruik gemaakt van zelfevaluaties.

Diverse informatiesystemen en verantwoording

Voorheen waren er aparte verantwoordingsprocedures voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Met ENSIA is dit nu gebundeld. 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.

In deze brief informeren wij u over de ENSIA auditresultaten.

Collegeverklaring informatiebeveiliging inzake DigiD en Suwinet

Uiterlijk 30 april 2019 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 Koninkrijksrelaties (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 in control is ten aanzien van 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 alle 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 bedoeld rapporten van bevindingen opgesteld. In deze rapporten van bevindingen zijn enkele aanbevelingen opgenomen om de kwaliteit van informatiebeveiliging nog verder te verbeteren.

Verantwoordingsrapportage BAG en BGT

In het kader van ENSIA hebben we in 2018 ook een zelfevaluatie uitgevoerd voor de BAG en de BGT. Deze zelfevaluatie gaat in op vier kwaliteitscriteria: borging proces, tijdigheid, volledigheid en juistheid. De resultaten uit deze zelfevaluatie zijn op 1 mei gedeeld met de toezichthouder (het ministerie van BZK) met een verantwoordingsrapportage BAG en een verantwoordingsrapportage BGT. Voor beide basisregistraties scoren we een voldoende, ruim 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 jaarverslag wordt er verantwoording afgelegd over informatiebeveiliging aan de gemeenteraad.

De collegeverklaring wordt gezamenlijk met het assurancerapport, maar zonder bijlagen, aangeboden aan de gemeenteraad. Op grond van artikel 25, tweede lid van de Gemeentewet, hebben we geheimhouding opgelegd op de collegeverklaring en bijlage 1 DigiD en bijlage 2 Suwinet van de collegeverklaring en het assurancerapport van de IT auditor. Uit vertrouwelijkheidsoogpunt zijn deze stukken op aanvraag in te zien.

Hoogachtend,

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

F.W. van Ardenne

A.J. Gerritsen