GEMEENTE MIDDEN-DRENTHE

Memo

Aan	College
Van	Jacobus Koops
Datum	30-05-2017
Zaaknummer	882922
Onderwerp	ENSIA

Wat is ENSIA?

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

Het project ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het verantwoordingsproces over informatieveiligheid bij gemeenten wordt hiermee verder geprofessionaliseerd door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan hier ook beter op sturen.

ENSIA helpt gemeenten in een keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Inkomen (SUWInet) is samengevoegd en gestroomlijnd.

Uitgangspunt is het horizontale verantwoordingsproces door het college van Burgemeester en Wethouders aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan de Ministeries die een rol hebben in het toezicht op informatieveiligheid.

Waarom ENSIA?

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de BIG als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Ook roepen de gemeenten in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. Dit was de aanleiding voor de start van het project ENSIA.

ENSIA is een initiatief van de VNG en de ministeries Binnenlandse Zaken en Koninkrijksrelaties, Infrastructuur en Milieu en Sociale Zaken en Werkgelegenheid.

Uit welke producten/onderdelen bestaat de ENSIA zelfevaluatie informatiebeveiliging voor de gemeente?

- **Vragenlijst zelfevaluatie informatiebeveiliging**
  Met de ingevulde zelfevaluatie vragenlijst en bijbehorende rapportages geeft het college van Burgemeester en Wethouders aan in hoeverre de beheersmaatregelen aan de beveiligingsnormen voldoen. Bij het opstellen van deze vragenlijst is vastgesteld waar de normen van BRP, PUN, DigiD, SUWInet, BAG en BGT aansluiten op de BIG-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIG-normen. Voor de specifieke normen van BRP, PUN, DigiD, SUWInet, BAG en BGT zijn aanvullende vragen geformuleerd.
- **Collegeverklaring ENSIA inzake informatiebeveiliging**
  Met deze verklaring geeft het college van Burgemeester en Wethouders aan in hoeverre bij de gemeente de beheersmaatregelen voldoen aan de voor de ENSIA verantwoording geselecteerde normen en indien aan de orde welke onderdelen daarvan zijn uitgezonderd. Ook wordt melding gemaakt van eventuele verbetermaatregelen die de gemeente gaat treffen. De Collegeverklaring wordt gezamenlijk met het Assurance rapport afzonderlijk van het jaarverslag aangeboden aan de gemeenteraad.
- **Assurance rapport**
  Een bij de Nederlandse Orde van Register EDP Auditors geregistreerde IT-auditor(NOREA geregistreerde IT-auditor) controleert de Collegeverklaring en stelt een Assurance rapport op. Deze werkzaamheden van de IT-auditor noemen we ook wel de IT-audit. De IT-auditor verklaart in het Assurance rapport dat de Collegeverklaring een getrouw beeld geeft. Dit betekent dat de Collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Kortom: deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de Collegeverklaring.
- **Paragraaf bedrijfsvoering in het jaarverslag wordt uitgebreid met een apart onderdeel over informatiebeveiliging**
  Het college van Burgemeester en Wethouders neemt in het jaarverslag in de paragraaf Bedrijfsvoering een aparte paragraaf op over informatiebeveiliging. Dit is conform de afspraak in de Resolutie informatieveiligheid: *“Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag”.*
  Deze paragraaf omvat informatie over de informatiebeveiliging in brede zin. Hierin rapporteert het college aan haar toezichthouder (de gemeenteraad) over informatiebeveiliging. Deze rapportage vloeit voort uit de afspraken in de gemeentelijke resolutie “Informatiebeveiliging randvoorwaarde voor een professionele gemeente”. De gemeenteraad stelt de jaarstukken, waaronder het jaarverslag, vast. In de paragraaf informatiebeveiliging verwijst het college naar de Collegeverklaring. De Collegeverklaring maakt geen deel uit van het jaarverslag. Om ongewenste samenloop met regelgeving voor accountants te voorkomen, is voorlopig gekozen voor het niet opnemen van de door IT-auditor gecontroleerde Collegeverklaring in het jaarverslag.

- **Rapportage BAG en BGT**
  Via de ENSIA-tooling stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie inclusief de Collegeverklaring en het Assurance rapport aan de minister van Binnenlandse Zaken en Koninkrijksrelaties ten behoeve van het toezicht op de BRP, de PUN en DigiD en aan de minister van Infrastructuur en Milieu ten behoeve van het toezicht op de BAG en BGT.
  De minister van Infrastructuur en Milieu dient de rapportages die in het kader van het toezicht op de BAG en BGT zijn aangeleverd te publiceren op www.basisregistratienm.nl. De conceptrapportages zijn beschikbaar via de ENSIA-tool en kunnen volgens instructie in de tool verder worden gecompleteerd en vastgesteld.

  Planning ENSIA-proces over het verantwoordingsjaar 2017
  Op hoofdlijnen verloopt de planning als volgt:
  1. Invullen en aanleveren zelfevaluatie vragenlijst (periode juli – december 2017).
     - Peildatum 1 oktober 2017: inleveren antwoorden die nodig zijn voor zelfevaluatie informatieveiligheid BRP en PUN.
     - Peildatum 31 december 2017: inleveren antwoorden die nodig zijn voor zelfevaluatie over de volle breedte van de BIG(dus met inbegrip van de zelfevaluatie DigiD, SUWInet, BAG en BGT) ten behoeve van de horizontale verantwoording informatieveiligheid aan de gemeenteraad.
  2. Opstellen en uploaden Collegeverklaring Informatiebeveiliging; uitvoeren van IT-audit en opstellen en uploaden van Assurance rapport (voor 1 mei 2018).
  3. Opstellen en uploaden rapportage BAG en BGT (voor 1 mei 2018).
  4. Het College van Burgemeester en Wethouders legt verantwoording af over informatieveiligheid, middels een paragraaf in jaarverslag. (Juli 1017)

Toelichting Ensia Midden-Drenthe 2017.
Van alle zelfevaluaties hebben we dit jaar twee verplicht moeten laten controleren. Dit betekent dat een onafhankelijke auditor van alle gestelde normen controleert of we voldoen (It-AUDIT). Voor 2017 waren dit zelfevaluaties DigiD en SUWInet. Op basis van de constateringen van de accountant stelt deze een Assurance verklaring op waarin verklaart wordt welke normen voldoen of niet voldoen. De auditor geeft de Assurance verklaring af op basis van een ondertekende collegeverklaring. De Ensia is nieuw met de gebruikelijke opstartproblemen en onduidelijkheden. Dit heeft ervoor gezorgd dat de afronding voor de deadline van 1 mei onder druk is komen te staan. Normaal gesproken zou de collegeverklaring eerst via een voorstel naar het college zijn gegaan om vervolgens na ondertekening deze naar de auditor te sturen. De auditor heeft geen aanbevelingen gedaan wat betekent dat we aan alle gestelde normen voldoen. Om deze redenen is er voor gekozen om de collegeverklaring eerst te laten ondertekenen en later aan te bieden bij het college. Voor 2018 betekend dit dat we de verplichte audits nog eerder gaan inplannen, om de zaken via het normale traject te kunnen afwikkelen.

Vervolgstappen.
De collegeverklaringen en assurance verklaringen voor de verplichte audits SUWInet en DigiD zullen alsnog aangeboden worden bij het college. Vervolgens worden deze ter informatie aangeboden bij de raad.