

Raadsinformatiebrief

Onderwerp

Informatiebeveiliging 2019

Datum

14-07-2020

Toelichting

In het kader van de ENSIA verantwoording 2019 is deze raadsinformatiebrief bedoeld om het verantwoordingstraject ENSIA en de uitkomsten hiervan uiteen te zetten, maar ook om de belangrijkste ontwikkelingen rondom informatiebeveiliging binnen de gemeente te delen.

Aanleiding

De gemeente verzamelt veel gegevens van o.a. burgers en bedrijven voor het uitvoeren van haar publieke taak. Burgers en bedrijven mogen van de overheid verwachten dat gegevens adequaat worden beveiligd.

Verantwoordingstraject ENSIA

Het project ENSIA is enkele jaren geleden opgezet om op een efficiënte en effectieve wijze verantwoording af te leggen over informatiebeveiliging. ENSIA staat voor Eenduidige Normatiek Single Information Audit en heeft als doel om eenduidig en door eenzelfde systematiek over verschillende onderdelen ten aanzien van informatieveiligheid verantwoording af te leggen.

De verantwoording vindt plaats aan de hand van het invullen van zelfevaluatievragenlijsten die gebaseerd zijn op het basisnormenkader voor informatiebeveiliging dat in 2019 voor het laatste jaar van kracht was; de Baseline Informatiebeveiliging Gemeenten (BIG). Door middel van zelfevaluatievragenlijsten wordt getoetst of aan de normen uit de BIG wordt voldaan. Daarbij wordt tevens getoetst of aan de verplichte beveiligingsnormen voor SUWI en DigiD wordt voldaan. Naast de zelfevaluatie bestaat de verantwoording uit een IT-audit op de collegeverklaring over DigiD en SUWI en een verantwoording in het jaarverslag (als onderdeel van de paragraaf Bedrijfsvoering). Het college legt horizontaal verantwoording af aan de raad en verticaal aan diverse ministeries en toezichtsorganen. We lichten de conclusies van deze zelfevaluatie over 2019 hieronder kort toe.

DigiD en Suwinet

Met DigiD kunnen burgers en bedrijven zich veilig digitaal identificeren bij overheidsorganisaties. Suwinet is een digitale infrastructuur waarin gegevens van burgers worden gedeeld tussen gemeenten, Belastingdienst, de SVB en het UWV voor het uitvoeren van hun wettelijke taak. Deze gegevens hebben betrekking op werk- en integratietrajecten, uitkeringen en opleidingen. Suwinet-taken worden uitgevoerd door de Gemeenschappelijke Regeling Peelgemeenten, maar de gemeente Laarbeek blijft eindverantwoordelijke voor de informatiebeveiliging. Het college verklaart met een collegeverklaring dat de gemeente voldoet aan de verplichte beheersmaatregelen met betrekking tot Suwinet. Er wordt nog niet volledig voldaan aan de verplichte beheersmaatregelen voor DigiD. De IT-audit en het daaruit voortvloeiende assurancerapport van de auditor bevestigen dit.

Voor DigiD is er daarom een verbeterplan opgesteld waarin verbetermaatregelen zijn opgenomen om alsnog volledig te voldoen aan de verplichte beheersmaatregelen. Deze verbetermaatregelen worden in het derde kwartaal van 2020 geïmplementeerd.

Basisregistraties in het GEO-informatiedomein

Het GEO-informatiedomein bestaat uit de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootchalige Topografie (BGT) en de Basisregistratie Ondergrond (BRO). De gemeente Laarbeek is als bronhouder verantwoordelijk voor het opnemen van gegevens in deze basisregistraties en de kwaliteit ervan. De BAG bestaat uit alle gemeentelijke gegevens omtrent adressen en gebouwen. Op basis van de zelfevaluatie geeft het college aan voor 88% te voldoen aan het normenkader (met een vereiste normgrens van 75%). De BGT is een digitale kaart van Nederland en daarin worden objecten als gebouwen, wegen, water, groen en spoorlijnen eenduidig vastgelegd. Op basis van de zelfevaluatie geeft het college aan voor 93% te voldoen aan het normenkader (met een vereiste normgrens van 75%). De BRO bevat gegevens over de geologische en bodemkundige opbouw van de Nederlandse ondergrond. De verantwoording over de BRO was in 2019 voor het eerst een verplicht onderdeel binnen de ENSIA-systematiek. Op basis van de zelfevaluatie geeft het college aan voor 42% te voldoen aan het normenkader (met een vereiste normgrens van 50%).

Voor de GEO-informatiedomeinen zijn verantwoordingsrapportages opgesteld met resultaten en eventuele verbeteracties. Deze rapportages worden via de ENSIA-tool ook opgestuurd naar de verticale toezichthouder; het Ministerie van BZK. De verbeteracties krijgen opvolging zodat volgend jaar wordt voldaan aan de dan geldende normgrens voor de BRO.

Een nieuwe basis voor informatiebeveiliging

De basis voor informatiebeveiliging was tot dit jaar het Basisnormenkader Informatiebeveiliging Gemeenten (BIG). In 2020 is de opvolger van de BIG van kracht gegaan, de Baseline Informatiebeveiliging Overheid (BIO). In de BIO is t.o.v. de BIG meer aandacht voor risicomanagement, lijnverantwoordelijkheid en het implementeren van verplichte

overheidsmaatregelen. Daarom zijn er in 2019 al enkele voorbereidende werkzaamheden uitgevoerd t.b.v. de voorbereiding op de BIO. Het belangrijkste was het starten met het schrijven van een nieuw informatiebeveiligingsbeleid voor 2020-2022.

Informatiebeveiligingsbeleid

In 2018 is door de rekenkamercommissie een onderzoek uitgevoerd naar de informatiebeveiliging in gemeente Laarbeek. Er is toen geconstateerd dat het huidige informatiebeveiligingsbeleid aan vervanging toe was. Aan de gemeenteraad is naar aanleiding daarvan toegezegd dat het beleid geactualiseerd zou worden. Met de komst van de BIO is nog meer de noodzaak ontstaan om het informatiebeveiligingsbeleid te vernieuwen. De meeste aanbevelingen van de Rekenkamercommissie betroffen onderdelen die ook in de BIO zijn opgenomen en zijn verwerkt in het nieuwe beleid. Het nieuwe informatiebeveiligingsbeleid 2020-2022 is op 14 juli 2020 door ons vastgesteld. In het informatiebeveiligingsbeleid 2020-2022 worden de ambitie en uitgangspunten van de gemeente op het gebied van informatiebeveiliging op strategisch niveau vastgelegd.

Informatiebeveiligingsorganisatie

De gemeente heeft een Chief Information Security Officer (CISO). De CISO voert tevens werkzaamheden uit voor de gemeente Gemert-Bakel en de Gemeenschappelijke Regeling Peelgemeenten. De CISO adviseert, controleert, ondersteunt en rapporteert (aan) het management op het gebied van informatiebeveiliging.

Bijlagen

N.v.t.

Hoogachtend,

Het college van burgemeester en wethouders,

gemeentesecretaris van Laarbeek,



J.W.M. van de Ven

de burgemeester van Laarbeek,



F.L.J. van der Meijden