Aan de gemeenteraad

Datum : 5 juli 2022
Zaaknummer : 674762
Contactpersoon : Annemieke Splithof
Telefoonnummer : 06 31 11 48 76

Onderwerp: ENSIA verantwoording 2021

Geachte voorzitter en leden,

Wij stellen u voor kennis te nemen van de Eenduidige Normatiek Single Information Audit (ENSIA) verantwoording op gebied van informatieveiligheid over het jaar 2021. Naast de ENSIA documentatie wenst de gemeenteraad ook inzage in het externe onderzoek naar het huidige volwassenheidsniveau op gebied van informatieveiligheid en privacy. Dit rapport is nog niet opgeleverd. Het zal naar verwachting deze zomer in het college worden vastgesteld. Hierna zal het onder geheimhouding met u worden gedeeld. Ook nodigen wij u uit om in besloten setting nadere toelichting te ontvangen over de ENSIA verantwoording van 2021 en het externe rapport dat nog volgt.

Inleiding

Het college van burgemeester en wethouders van de gemeente Arnhem legt over het jaar 2021 verantwoording af over de stand van zaken op het gebied van informatieveiligheid binnen de gemeentelijke organisatie. Dit gaat op basis van de landelijke ENSIA systematiek. Met deze nota legt het college verantwoording af aan de gemeenteraad omtrent de informatiebeveiliging van gemeente Arnhem in 2021.

We scoren onvoldoende op de ENSIA zelfevaluatie op de implementatie van de Baseline informatiebeveiliging Overheid (BIO) en op sommige andere onderdelen, zoals de Basisregistratie Ondergrond (BRO) en een tweetal aansluitingen op gebied van DigiD. Als college willen we voldoen aan de BIO en de andere ENSIA onderdelen. We constateren dat we daar nu nog niet aan voldoen en dat we nog veel werk te verzetten hebben om hieraan te gaan voldoen. Tegelijkertijd zien we de BIO als basis – een minimumset waaraan voldaan moet worden. In 2023 willen we daarom graag met u als raad bepalen hoe ver ons ambitieniveau als gemeente mag reiken als het gaat om informatieveiligheid bovenop het BIO-niveau.

Doelstelling

ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke planning & control-cyclus. Hierdoor heeft het

gemeentebestuur meer overzicht over en inzicht in de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen. ENSIA neemt de Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie.

Scope

De ENSIA verantwoording voor het jaar 2021 gaat over onderstaande onderdelen:

- Implementatie van de Baseline Informatiebeveiliging Overheid (BIO);
- Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet);
- Digitale Persoonsidentificatie (DigiD);
- Basis Registratie Personen (BRP);
- Paspoort Uitvoeringsregeling Nederland (PUN);
- Basisregistratie Grootschalige Topografie (BGT);
- Basisregistratie Adressen en Gebouwen (BAG);
- Basisregistratie Ondergrond (BRO);
- Waarderegistratie Onroerende Zaken (WOZ) (nieuw in de ENSIA verantwoording).

Specifiek voor de onderdelen DigiD en Suwinet is een assurance verklaring gevraagd van een onafhankelijke en geaccrediteerde auditor. Deze auditor toetst volgens de landelijke normenkaders over de opzet en het bestaan van beheersmaatregelen. Dit laatste wordt door de verticale toezichthouders Logius, BKWI en de Inspectie SZW vereist. De overige onderdelen bestaan uit een zelfevaluatie die betrokken medewerkers hebben uitgevoerd.

ENSIA verantwoording

Onderstaande tabel geeft per ENSIA-onderdeel een korte toelichting, bevindingen en de stand van zaken weer.

ENSIA Onderdeel	**Toelichting, bevindingen & stand van zaken**
Implementatie Baseline Informatieveiligheid Overheid (BIO)	De afgelopen jaren zijn veel stappen gezet op gebied van informatieveiligheid. Zo zijn er bijvoorbeeld CISO's (Chief Information Security Officers) aangenomen voor Arnhem en De Connectie en wordt er regionaal samengewerkt met Rheden en Renkum. De capaciteit op vlak van informatieveiligheid is echter nog beperkt, hierdoor kunnen sommige verplichte taken vanuit BIO en AVG niet worden uitgevoerd. Ook ten aanzien van bewustwording in de organisatie is verbetering nodig. Er worden activiteiten uitgevoerd maar nog op te beperkte schaal. Er is budget aangevraagd ten behoeve van een meerjarig verbeterprogramma Basis op orde. Het college onderschrijft de noodzaak om informatieveiligheid op orde te hebben en te voldoen aan de BIO. Informatieveiligheid wordt gezien als prioriteit daarom is de aanvraag van extra budget op gebied van informatieveiligheid en privacybescherming

	opgenomen in de begroting van het coalitieakkoord. Wanneer dit budget wordt toegekend zullen de te verbeteren punten projectgewijs worden opgepakt en verbeterd. De doorlooptijd hiervoor wordt ingeschat op 3 jaar.
Suwinet Structuur uitvoerings-organisatie Werk en Inkomen	Suwinet wordt gebruikt voor het uitvoeren van de participatiewet en adresonderzoeken door afdeling Burgerzaken. Vanwege de hoeveelheid en gevoeligheid van (persoons)gegevens binnen Suwinet heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties bepaald dat iedere aansluithouder naast de zelfevaluatie ook extern getoetst wordt op naleving van het normenkader. Het onderzoek van de externe auditor geeft aan dat de gemeente Arnhem voldoet aan de wettelijk gestelde eisen en normen in het kader van informatieveiligheid rondom het gebruik en beheer van alle Suwinet aansluitingen.
DigiD Digitale Persoons-identificatie	DigiD is voor inwoners de manier om zichzelf digitaal te identificeren. Onvoldoende of onjuist beheer van een DigiD aansluiting kan grote gevolgen hebben voor de landelijke keten en uiteindelijk persoonsinformatie van inwoners. Daarom heeft de toezichthouder bepaald dat iedere DigiD aansluiting naast een jaarlijkse zelfevaluatie ook (extern) getoetst wordt op naleving van het normenkader. Gemeente Arnhem maakt gebruik van vier DigiD aansluitingen. Twee van deze vier zijn uitstekend in orde. De derde is onvoldoende bevonden doordat onze leverancier op twee auditpunten onvoldoende heeft gescoord. Hierop is een verbetertraject ingezet. De vierde aansluiting is technisch en organisatorisch voldoende bevonden, echter hangt deze op de achtergrond aan hetzelfde aansluitnummer als aansluiting nummer drie. Hierdoor is ook de vierde aansluiting formeel afgekeurd. In 2022 zullen aansluiting drie en vier van elkaar ontkoppeld worden, waardoor het niet meer mogelijk is dat een aansluiting formeel wordt afgekeurd omdat hij hangt aan hetzelfde aansluitnummer als een aansluiting die onvoldoende presteert. De veiligheid van DigiD en websites staat onder druk. Het landelijke dreigingsbeeld geeft aan dat digitale risico's onverminderd groot zijn en cyberaanvallen steeds meer succesvol zijn met alle gevolgen van dien. De beveiliging vraagt steeds meer aandacht waarbij het een uitdaging is om dit huidige niveau vast te houden.
BRP Basis Registratie Personen	BRP is de basisregistratie waarin alle inwoners zijn geregistreerd. Gemeenten beheren deze BRP voor hun inwoners. Uiteindelijk worden alle BRP registraties landelijk gekoppeld zodat overheidsinstanties, zorgverleners en andere dienstverleners die gebruik mogen maken van deze BRP beschikken over de juiste persoonsinformatie. Vanwege het grote landelijke belang rondom de BRP zijn gemeenten verplicht om jaarlijks een

	zelfevaluatie uit te voeren. Afdeling Burgerzaken heeft in februari al hun eindrapportages met het college gedeeld, deze zijn gedeeltelijk gebaseerd op de Kwaliteitsmonitor en gedeeltelijk op ENSIA, en waren voldoende.
PUN Paspoort Uitvoeringsregeling Nederland	Gemeenten verzorgen de aanvraag en het uitreiken van reisdocumenten voor hun inwoners. Reisdocumenten zijn erg waardevol en vaak de sleutel van identiteitsfraude. De processen rondom het aanvragen en uitreiken zijn daarom strikt. Afdeling Burgerzaken heeft in februari al hun eindrapportages met het college gedeeld, deze zijn gedeeltelijk gebaseerd op de Kwaliteitsmonitor en gedeeltelijk op ENSIA. De zelfevaluatie PUN over het jaar 2021 is afgerond met een score van 100% De landelijke norm is minimaal 90%. Processen en de uitvoering rondom het aanvragen, beheren en uitreiken van reisdocumenten zijn uitstekend op orde.
BGT Basisregistratie Grootschalige Topografie	De BGT is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd. Kortom: de inrichting van de fysieke omgeving. De BGT is een landelijk uniforme registratie die alleen gemaakt kan worden vanuit een goede samenwerking tussen de diverse bronhouders. Gemeenten zijn als bronhouder mede verantwoordelijk voor de kwaliteit van deze landelijke basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BGT. De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 100%. Hiermee voldoen we aan de landelijk gestelde norm van 75%. In 2020 was de score 93%. Score 100% betekent niet dat er geen verbeteringen zijn. Er wordt continu gewerkt aan consistentie tussen de basisregistraties en optimaliseren van het proces hiervan.
BAG Basisregistratie Adressen en Gebouwen	De BAG bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Kopieën van al deze gegeven zijn verzameld in een landelijke voorziening. Deze voorziening wordt landelijk gebruikt door overheden, organisaties en particulieren. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BAG. De zelfevaluatie BAG over het jaar 2021 is afgerond met een score van 71%. Hiermee voldoen we net niet aan de landelijk gestelde norm 75%. In 2020 was de score 76%. De knelpunten zitten op de gegevenskwaliteit maar vooral op de tijdigheid. Dit werd veroorzaakt doordat onze ketenpartner de gegevens niet tijdig kon aanleveren, waardoor wij niet aan onze tijdigheid hebben kunnen voldoen.

	Inmiddels zijn hierover al afspraken gemaakt, waardoor de verwachting is dat de score voor 2022 weer voldoende zal zijn. Tevens zijn er door ons in 2021 een groot aantal mutaties fout opgevoerd. Dit heeft geleid tot een probleem in de gegevenskwaliteit. Betrokken medewerkers zijn inmiddels bijgeschoold, taken zijn anders verdeeld en er wordt consequent op kwaliteit gecontroleerd en gestuurd. De verwachting is daardoor dat de score op kwaliteit voor ENSIA 2022 weer voldoende zal zijn.
BRO Basisregistratie Ondergrond	De BRO bevat bodem- en ondergrondgegevens. Het gebruik van deze gegevens is de laatste decennia sterk toegenomen. Deze gegevens spelen een rol op uitvoerend niveau, maar zijn ook van belang bij het oplossen van maatschappelijke vraagstukken. Daarbij valt onder meer te denken aan het inpassen van de gevolgen van klimaatverandering zoals het stijgen van de zeewaterspiegel en bodemdaling. De gemeente is bronhouder voor deze basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BRO. De zelfevaluatie BRO over het jaar 2021 is negatief afgerond met een score van 11%, ruim onder de landelijk gestelde norm van 60%. De taken rondom het relatief nieuwe BRO proces zijn nog niet formeel belegd. Er worden stappen gezet om dit te formaliseren in de verwachting dat de score voor 2022 positiever zal zijn.
WOZ Waardebepaling Onroerende Zaken	Gemeenten en uitvoeringsorganisaties zullen bij de interne beheersing van risico's in het WOZ-proces voldoende aandacht moeten hebben voor de beheersing van geautomatiseerde systemen. Beheersingsaspecten die te maken hebben met architectuur, informatiebeveiliging, continuïteit, beschikbaarheid en algemene IT-beheersingsmaatregelen (General IT Controls als back-up & recovery, change management), moeten voldoende worden beheerst. Door snelle ontwikkelingen op het terrein van minimale beveiligingsmaatregelen en gewenste architectuur vergen deze aspecten even snel mee-ontwikkelende beheersingsmaatregelen. Om deze redenen is de WOZ verantwoording in 2021 toegevoegd aan de ENSIA zelfevaluatie. De meeste zaken binnen de WOZ zijn op orde. Wat niet op orde is, ligt in lijn met de verantwoording van de Baseline Informatieveiligheid Overheid (zie hierboven). De verwachting is dat, met het programma Basis op Orde, de kwaliteit van de zelfevaluatie WOZ voor 2022 zal verbeteren.

Hoogachtend,
het college van burgemeester en wethouders van Arnhem,
de secretaris, de burgemeester,

J.H. de Baas A. Marcouch

Bijlagen:

- Collegenota ENSIA 2021 (openbaar)

Geheim ter inzage voor de raad
- Rapportage stand van zaken informatieveiligheid 2021 (geheim, onbepaalde tijd)
- Collegeverklaring ENSIA 2021 (geheim, onbepaalde tijd)
- Rapport Gemeente Arnhem BAG BGT BRO (geheim, onbepaalde tijd)
- Rapport Gemeente Arnhem WOZ (geheim, onbepaalde tijd)

Motivatie geheimhouding:
Wettelijke bepaling:
Geheimhouding is opgelegd, overeenkomstig artikel 55 eerste lid van de Gemeentewet, op grond van artikel 10, tweede lid onder g van de Wet openbaarheid van bestuur, in verband met informatie over beveiligingsmaatregelen die de gemeente treft.

Inhoudelijke bepaling:
De onderliggende bijlagen bevatten informatie over aanbevelingen en maatregelen die de gemeente treft in het kader van informatiebeveiliging. Het is van belang dat deze documenten niet openbaar worden, omdat hierin informatie staat over de gemeentelijke informatiebeveiliging, die kwetsbaar wordt als derden (kwaadwillenden) hier inzage in krijgen. Zonder geheimhouding bestaat het risico dat de gemeente daardoor extra aantrekkelijk wordt voor hackers – we willen voorkomen dat we door openbaring een (grootschalige) hack zoals die bij Hof van Twente over onszelf afroepen. Daar niet duidelijk is wanneer de kwetsbaarheden zullen zijn opgelost, is de geheimhouding voor onbepaalde tijd, totdat alle issues zijn opgelost.