

VOORSTEL

zaaknummer: 1401380
afdelingsnaam: Interne Dienstverlening - IM
steller: Harriët Arnolds (ENSIA coördinator) en Jaap Huib van der Knaap (CISO)
telefoonnummer: 035 629 2912

onderwerp: ENSIA verantwoording gemeente Hilversum 2023

Voorstel

1. De collegeverklaring ENSIA 2023 en alle bijbehorende bijlagen vast te stellen;
2. De verklaring BAG, BGT, BRO en alle bijbehorende bijlagen vast te stellen;
3. De raad actief te informeren door middel van de bijgevoegde raadsinformatiebrief;
4. Krachtens artikel 87 van de Gemeentewet en artikel 5.1 lid 2 onder h van de Wet open overheid (belang van beveiliging van personen en bedrijven en het voorkomen van sabotage), de verplichting tot geheimhouding op te leggen voor informatie opgenomen in bijlage 4 tot en met 9 behorend bij dit voorstel. De verplichting tot geheimhouding wordt in acht genomen door allen die van de informatie kennis dragen.
5. Bijlage 4 tot en met 9 bij dit voorstel, onder verplichting tot geheimhouding te verstrekken aan de gemeenteraad conform artikel 88 lid 2 Gemeentewet.

Samenvatting

De Eenduidige Normatiek Single Information Audit (ENSIA) streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid binnen de Nederlandse overheid. Ook gemeenten verantwoorden zich middels deze audit over de staat van informatiebeveiliging binnen de eigen gemeente. Het doel van de ENSIA is het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). De basis van de ENSIA wordt gevormd door de [Baseline Informatiebeveiliging Overheid](#) (BIO). De Baseline beschrijft het basisniveau voor informatiebeveiliging dat wordt gehanteerd binnen de Nederlandse overheid.

De ENSIA (audit) is geënt op het een zo eenduidige en integraal mogelijke wijze van verantwoorden naar de daarvoor aangewezen verantwoordelijke instantie. Jaarlijkse voert de gemeente op haar landelijke voorzieningen deze audit uit. Per voorziening verschilt aan wie de gemeente verantwoording over de resultaten van de audit aflegt. Bij de ENSIA wordt gekeken naar informatiebeveiliging, maar voor diverse landelijke voorzieningen ook naar de data-kwaliteit en -integriteit.

De ENSIA-audit wordt toegepast voor de volgende gemeentelijke voorzieningen:

Voorziening	Component informatieveiligheid	Component Data-kwaliteit en -integriteit
Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).	✓	
Digitale persoonsidentificatie (DigiD),	✓	
Reisdocumenten (Paspoortuitvoeringsregeling Nederland (PUN)	✓	✓
Paspoorten en Nederlandse Identiteitskaarten (PNIK),	✓	✓
Basisregistraties		
Basisregistratie Adressen en Gebouwen (BAG)	✓	—
Basisregistratie Grootchalige Topografie (BGT)	✓	✓
Basisregistratie Ondergrond (BRO)	✓	— —
Basisregistratie Personen (BRP)	✓	✓

Conclusie component Informatieveiligheid

Over het afgelopen jaar **voldoen** we aan de informatiebeveiligingsnormen rondom DigiD en Suwinet voor alle voorzieningen en alle basisregistraties.

Conclusie component Data-kwaliteit en -integriteit

De conclusie is dat we **voldoen** aan de normen rondom kwaliteit van gegevens van de **BGT**, de **BRP**, en de **PUN/PNIK**.

Aan de gestelde eisen rondom de kwaliteit van de data **BAG** en de **BRO** wordt **niet volledig voldaan**.

De verbetering van de kwaliteit van de data in de BRO is noodzakelijk; de negatieve trend van de afgelopen jaren is nog niet gekeerd; het heeft vooral te maken met het verzamelen van data uit andere bronnen die door derden beheerd worden. Het College heeft reeds een eerste stap gezet door bij betreffende collega's en team(s) meer bewustwording te creëren.

Voor wat betreft de BAG is het verbeteren van de kwaliteit van de data nodig. Er zijn inmiddels acties ondernomen om dat te realiseren. Daarvoor zijn mensen en middelen ter beschikking gesteld.

De onderstaande verbeteringen zijn reeds doorgevoerd:

- Medewerkers in objectenbeheer zijn allround gemaakt (kwetsbaarheid is verminderd, waardoor tijdigheid, maar ook kwaliteit sterk verbeterd is);
- Kwaliteitsdashboard wordt dagelijks bijgehouden (voorheen niet geborgd).

We verwachten dat de maatregelen dit jaar leiden tot een verbetering van de gegevenskwaliteit.

Notabene

Het voorstel BRP PUN/PNIK wordt tegelijkertijd met deze stukken in het college aangeboden. Deze wordt daarna – zoals voorgeschreven - via de kwaliteitsmonitor van de stelselhouder aangeboden- en niet via de ENSIA systematiek. Voor het onderzoek naar de beveiligingsmaatregelen en de datakwaliteit treedt de burgemeester op als verantwoordelijk orgaan.

De verantwoording over het stelsel van de Waardering Onroerende Zaken (WOZ) – zoals u die vorig jaar aantrof in de ENSIA verantwoording - is door de Waarderingskamer weer uit het ENSIA verantwoordingsstelsel gehaald.

Inleiding

De verantwoording via ENSIA verloopt in vier fasen: zelfevaluatie, opstellen, verantwoorden en versturen.

Zelfevaluatie en opstellen

De ENSIA-coördinator heeft namens de gemeente de door de aangewezen instanties aangeboden vragenlijsten ingevuld in de ENSIA omgeving van de Rijksoverheid (vierde kwartaal 2023). De toezichthouder Bureau Keteninformatisering Werk en Inkomen (Suwinet) hanteert hiervoor de BIO-vragenlijst. Logius (DigiD) en ook Directoraatgeneraal Bestuur, Ruimte en Wonen van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BAG, BGT, BRO) hanteren hiervoor domeinspecifieke vragenlijsten.

In opstel-fase genereert de ENSIA-coördinator de verantwoordingsrapportages en vult deze aan. Voor DigiD en Suwinet stelt de ENSIA-coördinator een collegeverklaring op die door een auditor getoetst wordt.

Het resultaat van deze fase is een collegeverklaring voor DigiD en Suwinet, een rapportage over de BAG, BGT en BRO en een raadsinformatiebrief over ENSIA die aan de gemeenteraad wordt aangeboden. Voor de verantwoording BRP en Reisdocumenten (PUN/PNIK) treedt de burgemeester op als verantwoordelijk orgaan.

Verantwoorden en versturen

De fase Verantwoorden start op het moment dat de collegeverklaringen en de verantwoordingsrapportages door het college van B en W worden behandeld. Dit moet voor 30 april 2024 gebeuren. Het college B en W stelt de documenten vast en draagt zorg voor ondertekening. Daarna worden de rapportages in het landelijk ENSIA-systeem geüpload.

De vaststelling van de documenten voor de BRP en Reisdocumenten (PUN/PNIK) worden door PubliekZaken separaat ter tekening aangeboden. De rapportages (uittreksels) voor BRP en Reisdocumenten worden door hen daarna via de Kwaliteitsmonitor van Rijksdienst voor Identiteitsgegevens (RvIG) geüpload. Voor het aanleveren en ondertekenen van de uittreksel Reisdocumenten draagt de burgemeester verantwoordelijkheid.

Het resultaat van deze fase is dat de toezichthouders uiterlijk 30 april 2024 de gevraagde verantwoordingsrapportages ontvangen.

De concept collegeverklaring inzake DigiD en Suwinet zijn met bijbehorende stukken op 23 februari 2024 geaudit door een externe auditor. De auditor heeft hierover een assurance-verklaring afgegeven. Die assurance verklaring is noodzakelijk voor de continuering van de aansluitingen op DigiD en Suwinet.

Het gaat daarbij om de DigiD aansluitingen op:

- DigiD 1 - Sociaal Plein
- DigiD 2 - Belastingbalie
- DigiD 3 - Burgerzaken
- DigiD 4 - Zaaksysteem

Er liggen meerdere verklaringen voor ter vaststelling en/of ter ondertekening:

1. Collegeverklaring ENSIA 2023 inzake Informatiebeveiliging DigiD en Suwinet.
2. Verklaring ENSIA 2023 inzake BAG, BGT en BRO
3. Verantwoordingsrapportage 2023 BAG, BGT en BRO

De verklaringen en rapportages bestaan uit standaardteksten die niet aangepast mogen worden in de verantwoording naar de Rijksoverheid. In de Raadsinformatiebrief wordt uitleg gegeven over de manier waarop we informatiebeveiliging in Hilversum vormgeven; daar hebben we meer vrijheid in de manier waarop we informatiebeveiliging toelichten.

Doel

Het waarborgen van de informatiebeveiliging en (data) kwaliteit van bestaande voorzieningen / informatiesystemen en hierover de door de wet bepaalde verantwoording afleggen.

Argumenten

- 1.1. *De verklaringen en rapportages bestaan uit standaardteksten die niet aangepast mogen worden in de verantwoording naar de Rijksoverheid.*

Het college B en W heeft geen vrijheid om de verklaringen en rapportages aan te passen. De documenten dienen zonder enige aanpassing aangeboden te worden.

- 1.2. *De Gemeente Hilversum voldoet aan de vereiste normen voor DigiD en Suwinet.*

Wanneer het gaat over de Digitale persoonsidentificatie (DigiD), en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) geldt er een verzwaarde controle op de informatiebeveiliging en moet een externe auditor beoordelen of we de zaken op orde hebben. We verzamelen daarbij de Third Party Memoranda over de DigiD- en Suwinet aansluitingen. Tezamen met de door ons ingevulde ENSIA-vragenlijsten worden deze door de auditor beoordeeld, waarbij hij/zij de juistheid van de gegeven antwoorden vaststelt. Tenslotte controleert de externe auditor aan het einde van het proces nogmaals of alle stukken correct en volledig zijn voordat ze een officiële authenticatie van de auditor krijgen. De auditor heeft de controle op alle geleverde verklaringen rondom de DigiD aansluitingen en de Suwinet aansluitingen op 23 februari 2024 uitgevoerd en deze geauthentiseerd.

Over die audit geeft het college B en W vervolgens een collegeverklaring af, inclusief de onderliggende documenten zoals de Third Party Memoranda. Met het vaststellen van de bijbehorende collegeverklaring verklaart het college B en W in hoeverre de gemeente Hilversum voldoet aan de vereiste normen. Ook dit jaar voldoen we voor deze belangrijke aansluitingen aan alle gestelde informatiebeveiligingsnormen.

- 1.3. *Het aanbieden van de verklaring is nodig om de SUWI en DigiD -aansluitingen te continueren.* Niet ondertekenen zou betekenen dat de dienstverlening van de gemeente niet gecontinueerd kan worden omdat de stelselhouders de aansluitingen blokkeren. Bij blokkering van de toegang is dienstverlening aan inwoners en bedrijven niet meer mogelijk.

2. *De verklaring BAG, BGT, BRO en alle bijbehorende bijlagen vast te stellen om de dienstverlening te continueren;*

Het college B en W moet aan de stelselhouders verklaren dat het kennis genomen heeft van de situatie aangaande de verschillende stelsels. Op het gebied van informatiebeveiliging **voldoen we** voor alle basisregistraties aan de gestelde normen. De stelselhouders verplicht de vaststelling en ondertekening van de stukken om de dienstverlening te continueren. Ook hier geldt dat bij het niet aanbieden bijbehorende dienstverlening aan inwoners en bedrijven niet meer mogelijk is.

3. *Met de raadsinformatiebrief informeren wij de raad over de informatiebeveiliging van de DigiD en Suwinet aansluitingen en de gegevenskwaliteit van de basisstelsels.*

4. *Geheimhouding op onderliggende documenten (bijlagen) is noodzakelijk bij aanbieden aan de raad.* Op grond van het feit dat we geen inhoudelijke informatie over de stand van zaken van de informatiebeveiliging willen openbaren vragen wij het college B en W geheimhouding op de te leggen op de aangeboden bijlagen. Openbaarheid van de informatie inzake informatiebeveiliging van de systemen van de gemeente zou de positie van Hilversum kunnen schaden.

5. *De bijlagen 4 t/m 9 inzake ENSIA verantwoording 2023 bij dit raadsvoorstel, onder verplichting tot geheimhouding te verstrekken aan de gemeenteraad conform artikel 88 lid 2 Gemeentewet.*
Door verstrekking van de bijlagen kan de raad zich informeren over de stand van zaken rondom de informatiebeveiliging en datakwaliteit van de stelsels en aansluitingen.

Kanttekeningen

- 1.1. *We voldoen niet volledig aan de kwaliteit van de gegevens van de **BAG** en de **BRO** en daarvoor zijn in de stukken verbetermaatregelen opgenomen.*
We scoren net onder de norm voor de BAG en de BRO. Er is een verbeterplan opgesteld dat verschillende maatregelen omvat en er zijn mensen en middelen beschikbaar gesteld om dat te realiseren. Wij verwachten dat de maatregelen leiden tot een verdere verbetering van de gegevenskwaliteit. Het huidige niveau betekent niet dat we grote risico's lopen.
- 1.2. *De stelselhouders verplichten de vaststelling en ondertekening van de stukken om de dienstverlening te continueren.*
Hier geldt dat bij het niet aanbieden bijbehorende dienstverlening aan inwoners en bedrijven niet meer mogelijk is.

Financiën, middelen & capaciteit

Niet van toepassing.

Uitvoering

In de uitvoering kennen we de volgende stappen:

1. Het tekenen- en daarmee vaststellen - van de Collegeverklaring ENSIA 2023 inzake Informatiebeveiliging DigiD en Suwinet.
2. Het tekenen- en daarmee vaststellen van de Verklaring BAG, BGT en BRO en bijbehorende verantwoordingsrapportages 2023.
3. Na vaststelling van de collegeverklaring moet onze auditor de ondertekende collegeverklaring en bijbehorende bijlagen waarmerken en levert hij de assurance rapportage. Dit is een officiële – getekende verklaring van de auditor van de leverancier dat de beveiliging op de DigiD aansluiting voldoet.
4. Uiterlijk 30 april 2024 worden alle gewaarmerkte stukken door de ENSIA coördinator online verzonden naar ENSIA.
5. De stelselhouders continueren dan - na beoordeling - de aansluitingen van de gemeente Hilversum.

Bijlage(n)

1. 0402_Gemeente Hilversum_Collegeverklaring DigiD en Suwinet 2023_2023 ENSIA
2. Raadsinformatiebrief_ENSIA_Informatiebeveiliging_gemeente Hilversum 2023
3. 0402_Gemeente Hilversum_BAG-BGT-BRO 2023_2023 ENSIA

Niet openbare stukken (geheimhouding)

4. 0402_Gemeente Hilversum_Bijlage 1 DigiD 2023 - SaaS-leverancier_DigiD1_1005005_2023 ENSIA
5. 0402_Gemeente Hilversum_Bijlage 1 DigiD 2023 - SaaS-leverancier_DigiD2_1003403_2023 ENSIA
6. 0402_Gemeente Hilversum_Bijlage 1 DigiD 2023 - SaaS-leverancier_DigiD3_1003707_2023 ENSIA
7. 0402_Gemeente Hilversum_Bijlage 1 DigiD 2023 - SaaS-leverancier_DigiD4_1003789_2023 ENSIA
8. 0402_Gemeente Hilversum_Bijlage 2 Suwinet_2023 ENSIA
9. 0402_Gemeente Hilversum_BIO-rapportage 2023_2023 ENSIA