



Afdeling/eenheid/cluster: Advies	Projectnaam: Rapportage informatieveiligheid, Ensia-verantwoording en Zelfevaluatie BRP en PUN.	Bijl.: 7	Datum: 29 maart 2024	Steller: E Klompe
-------------------------------------	--	-------------	-------------------------	----------------------

Portefeuille: I

Onderwerp: Rapportage informatieveiligheid, ENSIA-verantwoording en de zelfevaluatie BRP en PUN 2023.

Voorgesteld besluit

1. Instemmen met en ondertekenen van de collegeverklaring ENSIA 2023 inzake DigiD en Suwinet.
2. Instemmen met en ondertekenen van de bestuursrapportages BAG, BGT en BRO, BRP en PUN.
3. Kennisnemen van de rapportage informatieveiligheid 2023.
4. De raad informeren via de rapportages en collegeverklaring.

Inleiding

Inwoners en ondernemers verwachten van de overheid dat zij zorgvuldig met hun gegevens omgaat. Dat betekent zorgen dat de gegevens betrouwbaar en beschikbaar zijn. Het betekent ook vertrouwelijk omgaan met die gegevens.

ENSIA¹ is door de VNG geïntroduceerd in 2017. Het doel is om als college in één keer verantwoording af te leggen over informatieveiligheid aan de gemeenteraad en aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen. De Wet Basisregistratie Personen (BRP) verplicht gemeenten om de inrichting, werking en beveiliging van de basisregistratie jaarlijks te evalueren. De paspoortuitvoeringsregeling Nederland (PUN) verplicht de burgemeester jaarlijks de inrichting, werking en de beveiliging van de reisdocumenten te evalueren. De verantwoording over 2023 vindt plaats volgens een vast patroon en met verplichte indeling en teksten² en moet vóór 30 april 2024 afgerond zijn.

Doelstelling

- Het college periodiek informeren over de status van onze informatieveiligheid.
- Verantwoording afleggen over de wijze waarop de gemeente voldoet aan kwaliteits- en informatieveiligheidsnormen van de Wet Basisregistratie Personen (BRP) en de Paspoort Uitvoeringsregeling Nederland (PUN).
- Invulling geven aan de landelijke afspraak over ENSIA waarmee uw college verantwoording richting de gemeenteraad en de verantwoording richting de Rijksoverheid (in hun rol als toezichthouder) over onze informatieveiligheid aflegt.

Argumenten

1.1. Gemeenten moeten verantwoording afleggen aan de Rijksoverheid via ENSIA.

Gemeenten moeten jaarlijks over informatieveiligheid rapporteren. Dit doen we door éénmalig een uitgebreide zelfevaluatielijst digitaal in te vullen in de ENSIA-tool. Hier wordt een verantwoordingsproces opgestart over:

- het voldoen aan de normen van de Baseline Informatiebeveiliging Overheid (BIO);
- de Digitale persoonsidentificatie (DigiD);

¹ Eenduidige Normatiek Single Information Audit

² Het niet gebruiken van het vaste format kan tot afkeuring van de documenten bij diverse ministeries leiden.

- de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- de Basisregistratie Adressen en Gebouwen (BAG);
- de Basisregistratie Grootchalige Topografie (BGT);
- de Basisregistratie Ondergrond (BRO);
- de Basisregistratie Personen (BRP);
- de Paspoortuitvoeringsregeling Nederland (PUN);

1.2. Uw college toont met de collegeverklaring aan dat de gemeente Noordoostpolder voldoet aan beveiligingsnormen voor DigiD en Suwinet.

- Inwoners kunnen hun zaken met de gemeente via ons Digitaal loket indienen. Er wordt met DigiD ingelogd. We moeten aan het ministerie van Binnenlandse Zaken en Koninkrijksrelaties aantonen dat wij voldoende preventie- en detectiemaatregelen nemen om veilig digitale dienstverlening te garanderen.
- We maken vooral bij het cluster Uitvoering Sociaal Domein gebruik van Suwinet. Zo kunnen we persoonsgegevens van inwoners, die bij verschillende organisaties of basisregistraties zijn opgeslagen, raadplegen in één web toepassing. Als afnemer Suwinet moeten we aantonen dat we de veiligheid van de persoonsgegevens voldoende waarborgen.

We tonen dit aan via een collegeverklaring die door een EDP-auditor is gecontroleerd en gewaarmerkt.

2.1. Uw college toont via de bestuursrapportage voor de BAG, BGT en BRO aan in welke mate we voldoen aan de kwaliteitsnormen.

Als gemeente zijn we bronhouder van de BAG, BGT en BRO. We moeten jaarlijks zelfevaluaties uitvoeren. Deze evaluaties betreffen de gegevenskwaliteit en de borging van beheerprocessen. Via de bestuursrapportage tonen we aan het ministerie van Binnenlandse Zaken en Koninkrijksrelaties aan dat we voldoen aan de kwaliteitscriteria voor de basisregistraties. De trend van de laatste vier jaar laat zien dat de basisregistraties op orde zijn. In de rapportage wordt in hoofdstuk 3 ingegaan op de stand van zaken verbeterplan 2022 en zijn naar aanleiding van de bevindingen 2023 nieuwe verbetermaatregelen geformuleerd.

2.2 Uw college toont via het uittreksel BRP en het uittreksel Reisdocumenten (PUN) aan in welke mate we voldoen aan de kwaliteitsnormen.

Op grond van artikel 4.3 van de wet BRP verricht het college van burgemeester en wethouders periodiek een onderzoek naar de inrichting, de werking en de beveiliging van de basisregistratie personen en naar de verwerking van gegevens in de basisregistratie. Op grond van artikel 94.1 van de PUN wordt periodiek controle uitgevoerd op de toepassing van de beveiligingsmaatregelen. Voor beide regelingen geldt dat daarbij gebruik moet worden gemaakt van de daarvoor door de Minister van Binnenlandse Zaken en Koninkrijksrelaties beschikbaar gestelde hulpmiddelen. Dat betekent beantwoording van een vragenlijst in de Kwaliteitsmonitor en de ENSIA-tool. Voor de BRP vindt daarnaast ook een bestandscontrole en een inhoudelijke controle op de persoonslijsten plaats. De resultaten, detailinformatie en verbeterpunten, zijn in de vorm van een uittreksel en een managementrapportage aan de gemeente beschikbaar gesteld. Verbeterpunten uit de Kwaliteitsmonitor en de Ensia-verantwoording BRP en Reisdocumenten worden opgepakt door de werkgroep die ook de actualisering van het informatiebeveiligingsplan Klant Contactcentrum inclusief alle bijbehorende werkprocessen oppakt. Deze actualisering is noodzakelijk omdat op 24 november 2023 het Klant Contactcentrum (KCC) de overstap heeft gemaakt van Key2Burgerzaken naar iBurgerzaken.

3.1. In het strategisch informatieveiligheidsbeleid is vastgelegd dat jaarlijks gerapporteerd wordt over informatieveiligheid aan uw college.

Het college heeft een coördinator informatiebeveiliging benoemd die onafhankelijk adviseert en signaleert over informatieveiligheid. Deze functionaris stelt jaarlijks een rapportage informatieveiligheid op. Als bijlage bij dit voorstel treft u deze rapportage aan.

4.1. Uw college legt verantwoording af over informatieveiligheid aan de gemeenteraad.

Inwoners en ondernemers verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van

informatie(systemen). Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college jaarlijks verantwoording over informatieveiligheid aflegt aan de gemeenteraad. Dit doen we via het hoofdstuk informatieveiligheid en privacy in de paragraaf bedrijfsvoering van het jaarverslag 2023. Aanvullend worden dit collegevoorstel, de rapportage informatieveiligheid en de collegeverklaring ter informatie aan de gemeenteraad verstrekt. Dit zonder bijlagen vanwege het vertrouwelijk karakter³ daarvan.

Kanttekeningen

1.1 De verschillende rapportages zijn bestemd voor specialisten en daardoor gedetailleerd en volgens een vast format.

De verantwoording richting de verschillende Rijksoverheden wordt getoetst door specialisten. Dat betekent dat de bijlagen bij dit voorstel soms gedetailleerde informatie bevatten en volgens een vast (verplicht) format zijn weergegeven. Essentie voor uw college is dat de bijlagen aantonen dat de gemeente voldoende maatregelen treft om te zorgen dat de gegevens in de bronregistraties voldoende beschermd zijn en dat de kwaliteit van gegevens gewaarborgd is.

Planning/Uitvoering

- Na behandeling in de collegevergadering wordt de collegeverklaring door uw college getekend.
- De gewaarmerkte collegeverklaring, een Assurance verklaring, en de bestuursrapportages BAG, BGT, BRO en WOZ worden geüpload in de ENSIA-tool voor de verantwoording richting de Rijksoverheid.
- Na behandeling in de collegevergadering wordt het uittreksel BRP door uw college getekend en het uittreksel PUN door de burgemeester. Deze worden geüpload in de Kwaliteitsmonitor voor de verantwoording aan de Rijksdienst voor Identiteitsgegevens (RvIG) en de Autoriteit Persoonsgegevens (AP).
- Het collegevoorstel, de rapportage informatieveiligheid en de collegeverklaring worden ter informatie aan de gemeenteraad verstrekt.
- Daar waar in managementrapportages of Assurance rapporten verbeter suggesties zijn opgenomen, wordt aan de verantwoordelijke managers gevraagd deze maatregelen op te pakken. De Ensia coördinator en de coördinator informatiebeveiliging zien hierop toe.

Bijlagen

- Rapportage informatieveiligheid 2023
- Collegeverklaring
- Bijlage 1 collegeverklaring DigiD
- Bijlage 2 collegeverklaring Suwinet
- Bestuursrapportage BAG, BGT en BRO
- Uittreksel Reisdocumenten 2023
- Uittreksel BRP 2023

³ De Informatiebeveiligingsdienst voor gemeenten (IBD) heeft gemeenten nog eens nadrukkelijk gewezen op vertrouwelijkheid van de bijlagen, deze bevat gegevens die door kwaadwillende misbruikt zouden kunnen worden.