

| | |
|----------|---|
| Aan: | Gemeenteraad van de gemeente Tilburg |
| Van: | College van burgemeester en wethouders |
| Betreft: | Stand van zaken informatieveiligheid 2019 |
| Datum: | 14 april 2020 |

Inleiding

Het college van burgemeester en wethouders van de gemeente Tilburg legt over het jaar 2019 verantwoording af over de stand van zaken op het gebied van informatieveiligheid binnen de gemeentelijke organisatie. Dit gaat op basis van de landelijke Eenduidige Normatiek Single Information Audit (= ENSIA) systematiek.

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 de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen. ENSIA neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie.

Scope

De ENSIA verantwoording voor het jaar 2019 gaat over onderstaande onderdelen:

- Implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG);
- Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet);
- Digitale Persoonsidentificatie (DigiD);
- Basis Registratie Personen (BRP);
- Paspoort Uitvoeringsregeling Nederland (PUN);
- Basisregistratie Grootchalige Topografie (BGT);
- Basisregistratie Adressen en Gebouwen (BAG);
- Basisregistratie Ondergrond (BRO);





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.




Voor de leesbaarheid is per onderdeel met behulp van smiley's de status per onderdeel weergegeven. Per onderdeel zijn ook de bevindingen kort uitgewerkt ter onderbouwing van deze status.


Legenda:

|  |  |  |  |
|---|---|--|--|
| <i>Ruim voldoende tot Goed</i> | <i>Voldoende</i> | <i>Net Onvoldoende</i> | <i>Onvoldoende</i> |
| Het onderdeel is volledig op orde, in control Wellicht zijn er minimale verbeterpunten | Het onderdeel is globaal op orde in control Er zijn enkele verbeterpunten | Het onderdeel is net niet in control Er zijn meerdere verbeterpunten | Het onderdeel is niet in control Er zijn veel verbeterpunten, bijsturing is nodig |

| ENSIA Onderdeel | Toelichting, bevindingen & stand van zaken | Status |
|---|--|---|
| Implementatie Baseline Informatiebeveiliging Gemeenten (BIG) | <p>Gemeente Tilburg is al enkele jaren bezig met de implementatie van de BIG. Veel (landelijk voorgestelde) beheersmaatregelen zijn bij ons reeds geïmplementeerd. Vanaf 2020 is de BIG vervangen door de Baseline Informatiebeveiliging Overheid (BIO). Deze BIO is nu voor de gehele overheid het normenkader en geeft organisaties meer ruimte om op basis van een eigen risico afweging keuzes te maken in het implementeren van beheers- en beveiligingsmaatregelen. Hierbij blijft een basis pakket aan generieke maatregelen voor iedere (overheid)organisatie verplicht.</p> <p>De implementatie van de nieuwe BIO doen we in afstemming en samenwerking met de Brabantse 5 (grootste) gemeenten. We starten met een nieuw informatiebeveiligingsbeleid wat kaders en richting geeft aan de organisatie.</p> <p>Informatieveiligheid is veel meer dan het implementeren van technische maatregelen. Uit verschillende dreigingsbeelden blijkt dat het bijna altijd mis gaat door (onbewust) menselijk handelen. Bewuste medewerkers zijn de beste beveiligingsmaatregel.</p> <p>In 2019 is intern hard gewerkt aan het bewuster en weerbaarder maken van onze medewerkers op het gebied van informatieveiligheid en privacy. De campagne bestond uit algemene activiteiten zoals communicatie uitingen, lezingen en een cybersecurity Escaperoom. Daarnaast waren er ook activiteiten waarin medewerkers werden geconfronteerd (het overkomt je) zoals een Phishingtest, Mystery guest onderzoek en Clean desk controle.</p> <p>Uit de (ENSIA) zelfevaluaties blijkt dat informatieveiligheid binnen onze organisatie voldoende is geborgd. Het blijven ontwikkelen en werken aan onze weerbaarheid is een continu proces.</p> |  |
| Suwinet Structuur uitvoerings-organisatie Werk en Inkomen | <p>Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet, adresonderzoeken (ter verbetering van de Basis Registratie Personen) en voor het heffen van belastingen. Iedere taak gebruikt een aparte Suwinet aansluiting.</p> <p>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.</p> <p>Het onderzoek van de externe auditor geeft aan dat de gemeente Tilburg voldoet aan de wettelijk gestelde eisen en normen in het kader van informatieveiligheid rondom het gebruik en beheer van alle Suwinet aansluitingen.</p> |  |
| DigiD Digitale Persoons-identificatie | <p>DigiD is voor inwoners de manier om zichzelf digitaal te identificeren. DigiD wordt gebruikt voor de digitale dienstverlening via onze website/winkel Tilburg.nl. Ontwikkeling en het beheer van Tilburg.nl is volledig binnen de eigen organisatie ondergebracht.</p> <p>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</p> | |

| | | |
|--|--|---|
| | <p>jaarlijkse zelfevaluatie ook (extern) getoetst wordt op naleving van het normenkader.</p> <p>Het onderzoek van de externe auditor geeft aan dat onze processen rondom DigiD op orde zijn. Wij voldoen voor onze website/webwinkel Tilburg.nl aan de gestelde informatiebeveiligingsnormen.</p> <p>Naast het onderzoek rondom organisatorische waarborgen heeft er ook een technische penetratietest plaatsgevonden op Tilburg.nl. Ook deze uitkomst is positief, er zijn geen kwetsbaarheden ontdekt.</p> |  |
| <p>BRP</p> <p>Basis Registratie Personen</p> | <p>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.</p> <p>Deze zelfevaluatie bestaat uit 3 onderdelen.</p> <p>1. Een bestandscontrole op de persoonslijsten.</p> <p>Bij de bestandscontrole van 05-12-2019 zijn de persoonslijsten gecontroleerd, waarvan 99,88 % van de actuele persoonslijsten als correct is bevonden. Dit voldoet ruimschoots aan norm.</p> <p>2. Een inhoudelijke controle van persoonslijsten.</p> <p>Aan de hand van brondocumenten is een controle uitgevoerd naar de juiste verwerking daarvan in de basisregistratie. De resultaten hiervan voldoen op 4 van de 7 getoetste klassen niet aan de norm. Dit is lichte een verbetering ten opzichte van vorig jaar toen nog op 5 van de getoetste klassen niet werd voldaan aan de norm. De steekproef wordt uitgevoerd aan de hand van brondocumenten die in de afgelopen 10 jaar in de BRP zijn opgenomen. Verbeteringen in het proces en kwaliteit zijn daardoor pas langzaam zichtbaar en hebben geen directe invloed op persoonslijsten uit het verleden. Sinds vorig jaar is ingezet op een intensieve controle van de mutaties in de BRP zodat fouten nu tijdig opgemerkt en gecorrigeerd worden. Deze controles worden gecontinueerd.</p> <p>3. Een controle op uitvoering van de processen.</p> <p>Door middel van een vragenlijst is dit onderdeel onderzocht. In de vragenlijst staan vragen over de procedures die gevolgd worden bij het verwerken en beveiligen van persoonsgegevens.</p> <p>De gemeente scoort 88,9%. Dit is volgens de landelijke gestelde norm van 90% nog "net" onvoldoende. Ten opzichte van vorig jaar (83,3%) is dit wel een flinke verbetering. Op alle onderdelen is de score verbeterd.</p> <p>Voor het onderdeel "processen" scoort burgerzaken goed en liggen verbeterpunten voornamelijk generiek (organisatie breed). Dit gaat dan over het op orde brengen van autorisaties, periodieke controles van autorisaties en systemen en databescherming zoals dataclassificatie.</p> <p>De impact voor onze inwoners is niet direct kritisch of zichtbaar. Later bij bijvoorbeeld het aanvragen van een reisdocument of uittreksel komen dit soort</p> |  |

| | | |
|---|--|---|
| | <p>fouten uit. Op dat moment is dit vervelend omdat de inwoner geconfronteerd wordt met onjuiste gegevens en dit op dat moment eerst gecorrigeerd moet worden door de medewerker .</p> <p><i>Het resultaat van de zelfevaluatie BRP is in februari besproken in het college. Voor de BRP is in 2019 een verbeterplan opgesteld en in uitvoering. Verbeteringen zijn in de resultaten al zichtbaar. Doel is om in de komende zelfevaluatie op het onderdeel processen voldoende te scoren. De kwaliteit slag binnen de inhoudelijke BRP vraagt een langer traject.</i></p> | |
| PUN Paspoort Uitvoeringsregeling Nederland | <p>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. De burgemeester is verantwoordelijk voor de borging van deze processen en moet hierover jaarlijks verantwoording afleggen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties. Via de ENSIA verantwoording infomeren we ook het eigen bestuur over de stand van zaken.</p> <p>De zelfevaluatie PUN over het jaar 2018 is afgerond met een score van 92,4% De landelijke norm is minimaal 90%. Hiermee is het eindresultaat "ruim voldoende". Processen en de uitvoering rondom het aanvragen, beheren en uitreiken van reisdocumenten zijn op orde.</p> |  |
| BGT Basisregistratie Grootchalige Topografie | <p>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.</p> <p>De zelfevaluatie BGT over het jaar 2019 is afgerond met een score van 130 van maximaal 150. Hiermee voldoen we aan de landelijk gestelde norm van 113. In 2018 was de score 125.</p> <p>Gemeente Tilburg gebruikt de BGT niet als bronbestand, maar genereert de BGT vanuit een geometrische bron-dataset: KernRegistratie Topografie (KRT). De Kernregistratie Topografie is de centrale registratie waarin alle geometrische objecten middels een regelgeving geïntegreerd beheerd worden. Vanuit de KRT worden alle afnemende registraties zoals BAG, BGT, en BOR voorzien van de juiste geometrische objecten. De interne (bijhoudings)processen zijn zo ingericht dat we voldoen aan de eisen en verplichtingen die de wet BGT voorschrijft.</p> |  |
| BAG Basisregistratie Adressen en Gebouwen | <p>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.</p> <p>De zelfevaluatie BAG over het jaar 2019 is afgerond met een score van 195 van maximaal 205. Hiermee voldoen we ruim aan de landelijk gestelde norm van 154.</p> |  |

| | | |
|---|---|---|
| | <p>In 2018 was de score 205.</p> <p>Er is sprake van een goed lopend proces, waarbij periodiek afstemming plaatsvindt tussen belangrijke leveranciers van informatie (zoals omgevingsvergunningen en Geo-Informatie) en afnemers van onze basisgegevens.</p> <p>De kwaliteit van de gegevens verbetert door tijdens het gebruik eventuele fouten en/of afwijkingen terug te melden.</p> | |
| BRO Basisregistratie Ondergrond | <p>De BRO bevat bodem- en ondergrondgegevens. Het gebruik van deze gegevens is de laatste decennia sterk toegenomen. Deze gegevens spelen een cruciale 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.</p> <p>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.</p> <p>De zelfevaluatie BRO over het jaar 2019 is afgerond met een score van 40 van maximaal 120. Dit is onder de gestelde norm van 72 voor een positief resultaat.</p> <p>Een goede informatievoorziening over de ondergrond is van wezenlijk belang voor het realiseren van bestuurlijke ambities als het omgevingsplan, de energietransitie, watertoets en dergelijke. Als we willen dat de burger hier ook actief in participeert, moet het fundament hiervoor op orde en goed ingevuld zijn. De BRO is een van de elementen die de verschillende opgaves mogelijk moeten maken.</p> <p>Voor de BRO is in 2019 een implementatie project gestart. Dit heeft nog niet tot gewenste en noodzakelijke resultaten geleid. In 2020 zal er echt doorgepakt worden op de implementatie van de BRO zodat we bij een volgende zelfevaluatie aan de minimaal gestelde normen voldoen. Het uitgangspunt hierbij is om het beheer en de kwaliteit op eenzelfde niveau te brengen als de BAG en BGT.</p> <p>Afspraak is dat het college na het 2^e kwartaal van 2020 zal worden geïnformeerd over de stand van zaken met betrekking tot ingezette verbeteracties.</p> |  |