

Raadsinformatiebrief

Aan Raad
Portefeuillehouder Mark van Stappershoef
Onderwerp Stand van zaken informatieveiligheid 2020
Datum 14-04-2021

Kennisnemen van

De stand van zaken op het gebied van Informatieveiligheid en Privacy binnen de gemeente Goirle.

Inleiding

De gemeente Goirle wil een betrouwbare organisatie zijn voor inwoners, (keten)partners en bedrijven. Ons informatiebeveiligingsbeleid geeft kaders, richting en sturing. Dit vertalen we naar te nemen maatregelen om onze informatievoorziening en vertrouwelijke informatie te beschermen en misbruik te voorkomen. Hiermee dragen we bij aan een weerbare overheid.

Met de rapportage geven we inzicht in, en leggen we verantwoording af over de stand van zaken op het gebied van informatieveiligheid binnen onze organisatie.

Het college van burgemeester en wethouders van de gemeente Goirle legt over het jaar 2020 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.

Deze ENSIA-verantwoording is voor gemeenten verplicht en is ingericht om verantwoording af te leggen aan de gemeenteraad (horizontale verantwoording) en aan de verschillende toezichthouders (verticale verantwoording). Verantwoording afleggen aan onze gemeenteraad doen we in de vorm van een raadsinformatiebrief.

ENSIA sluit aan op de gemeentelijke planning en control cyclus voor informatiebeveiliging, neemt de landelijke Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

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.

Uit de verschillende zelfevaluaties en de externe audit blijkt dat gemeente Goirle informatiebeveiliging over het geheel gezien voldoende heeft geborgd. Er zijn verbeterpunten die opgepakt worden en waarbij de voortgang bewaakt wordt.

DigiD Zaaksysteem:





Het DigiD onderdeel binnen ons zaaksysteem voldoet op dit moment nog niet aan de nieuw gestelde eisen voor DigiD. De oorzaak hiervan heeft te maken met een aanscherping op het normenkader. Deze aanscherping is nodig om digitale dreigingen te blijven ondervangen. De leverancier is druk bezig om deze omgeving als nog aan het nieuw gestelde beveiligingsniveau te laten voldoen. Het risico voor onze inwoners is op dit moment zeer beperkt.

Informatie

Onderstaande tabellen geven 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 weergegeven. Per onderdeel zijn ook de bevindingen kort uitgewerkt ter onderbouwing van deze status.


In de rapportage is extra aandacht besteed aan de privacy waarborging van inwoners en medewerkers (AVG).

Legenda:

			
Ruim voldoende tot goed	Voldoende	Onvoldoende	In voorbereiding
Het onderdeel is op orde, in control. Wellicht zijn er minimale verbeterpunten.	Het onderdeel is globaal op orde (net) in control. Er zijn enkele verbeterpunten.	Het onderdeel is niet in control. Er zijn meerdere verbeterpunten, bijsturing is nodig.	Het onderdeel is in voorbereiding. Er is nog niet gestart met de implementatie. Deze is wel gepland.




Tabel 1 geeft toelichting over de verantwoording Baseline Informatiebeveiliging Gemeenten (BIO) en de wet Algemene Verordening Gegevensbescherming (AVG)





Domein	Stand van zaken	Status
BIO Waarborgen van informatie-veiligheid	De BIO is vanaf 2020 voor de gehele overheid het normenkader in het kader van informatiebeveiliging. Deze BIO 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 basispakket aan generieke maatregelen voor iedere (overheid)organisatie verplicht. Gemeente Goirle is in 2020 gestart met de implementatie van de BIO. Veel maatregelen zijn gelijk aan het vorige normenkader en waren eerder al (deels) geïmplementeerd.	

	<p>Een belangrijke stap is het bestuurlijk vaststellen van een informatiebeveiligingsbeleid. Dit is inmiddels gedaan en geeft onze organisatie kaders en richting om op het gebied van informatieveiligheid weerbaarder te worden en dat ook te blijven.</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>Rondom bewustwording is vanwege Covid-19 de focus verplaatst naar het (digitaal) veilig op afstand werken. Collega's zijn op verschillende manieren bewust gemaakt van de risico's en mogelijkheden die dit nieuwe werken met zich meebrengt.</p> <p>Verder is informatieveiligheid binnen onze organisatie voldoende geborgd. Dit blijkt uit de (ENSIA) zelfevaluaties en voor een aantal domeinen uit de externe audits. Het blijven ontwikkelen en werken aan onze weerbaarheid is een continu proces en vraagt ook altijd om aandacht.</p>	
<p>AVG</p> <p>Waarborgen rondom privacy van inwoners en medewerkers</p>	<p>In Goirle is de door de AVG vereiste privacy administratie (denk hierbij aan het register van verwerkingsactiviteiten, register van incidenten en datalekken, etc.) bijna volledig op orde. De laatste stappen op dit gebied zullen we begin 2021 afronden. Een goede, duidelijke en actuele basis is essentieel om de komende jaren planmatig en continu te gaan werken aan gerichte verbetering van alle processen binnen de gemeente. Hierbij trekken Informatieveiligheid en privacy samen op en wordt er gebruik gemaakt van een managementsysteem.</p> <p>Privacy is inmiddels geborgd in tal van processen waaronder inkoop en aanbesteding. De gevraagde en ongevraagde adviezen vanuit privacy geleid tot aanpassing van tal van processen en werkwijzen en is de uitwisseling van persoonsgegevens binnen GHO geborgd.</p> <p>Bewustwording</p> <p>Zoals aangegeven bij de BIO ligt onze focus de gehele beleidscyclus op het creëren van meer bewustwording in de organisatie. Daarnaast is geïnvesteerd in een veilige meldcultuur waarin het melden van beveiligingsincidenten en datalekken wordt beloond. We proberen mee te denken met medewerkers, door te denken in mogelijkheden in plaats van beperkingen. Door Covid-19 is er meer gewerkt aan bewustwording rondom veilig thuiswerken. Begin 2021 is gestart met een inhaalslag op het gebied van bewustwording</p>	

Verantwoording per onderdeel ENSIA-domein specifiek

Tabel 2 geeft per domein een korte toelichting, bevindingen en de stand van zaken weer.

Domein	Toelichting, bevindingen & stand van zaken	Status
<p>Suwinet</p> <p>Structuur uitvoeringsorganisatie</p> <p>Werk en Inkomen</p>	<p>Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet en adresonderzoeken (ter verbetering van de Basis Registratie Personen). 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 Goirle voldoet aan de wettelijk gestelde eisen en normen in het kader van informatieveiligheid rondom het gebruik en beheer van alle Suwinet aansluitingen.</p>	
<p>DigiD</p> <p>Digitale Persoons-identificatie</p> <p>Zaaksysteem</p>	<p>DigiD is voor inwoners de manier om zichzelf digitaal te identificeren en wordt gebruikt voor de digitale dienstverlening via onze website. 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.</p> <p>Ontwikkeling en het beheer van ons zaaksysteem is grotendeels uitbesteed. Het functioneel beheer is intern geregeld.</p> <p>Onze externe beheerder voldoet op dit moment voor één norm niet aan het gestelde kader voor een veilige omgeving. Reden hiervan is een recente aanscherping op deze technische norm. De leverancier heeft een verbeterplan opgesteld om alsnog aan deze nieuwe gestelde eisen te gaan voldoen. Deze aanpassingen zijn voor 1 november 2021 ingevoerd.</p> <p>Het onderzoek van onze externe auditor geeft aan dat onze processen rondom DigiD op orde zijn. Wijzelf voldoen aan de gestelde informatiebeveiligingsnormen.</p>	
<p>DigiD</p> <p>Digitale belastingbalie</p>	<p>Ontwikkeling en het beheer van onze digitale belastingbalie is volledig uitbesteed.</p> <p>Zowel bij de leverancier als bij onszelf heeft een extern onderzoek plaatsgevonden. Het resultaat hiervan is positief. We voldoen aan de gestelde informatiebeveiligingsnormen voor een veilige DigiD omgeving.</p>	

<p>BRP</p> <p>Basis Registratie Personen</p>	<p>De 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>De zelfevaluatie BRP (processen en uitvoering) over het jaar 2020 is afgerond met een score van 99,6%. Dit zit ruim boven de landelijk gestelde norm van 90%.</p> <p>Inhoudelijke BRP: Ook de inhoudelijke controle op de kwaliteit van onze Basis Registratie Personen is over het jaar 2020 positief afgerond.</p>	
<p>PUN</p> <p>Paspoort Uitvoerings- regeling Nederland</p>	<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 2020 is afgerond met een score van 99%. De landelijke norm is minimaal 90%. Hiermee is het eindresultaat "zeer goed". Processen en de uitvoering rondom het aanvragen, beheren en uitreiken van reisdocumenten zijn goed op orde.</p>	
<p>BGT</p> <p>Basisregistratie Grootschalige Topografie</p>	<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 medeverantwoordelijk 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 2020 is afgerond met een score van 150 van maximaal 150. Hiermee voldoen we aan de landelijk gestelde norm van 113. In 2019 was de score 125.</p>	
<p>BAG</p> <p>Basisregistratie Adressen en</p>	<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</p>	

Gebouwen	<p>bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BAG.</p> <p>De zelfevaluatie BAG over het jaar 2020 is afgerond met een score van 165 van maximaal 205. Hiermee voldoen we aan de landelijk gestelde norm van 154. In 2019 was de score 200.</p> <p><i>Door een vertraging in het interne bijhoudingsproces scoren we in 2020 minder goed op het gebied van actualiteit. Inmiddels houden we een logboek bij en overleggen we periodiek met de afdeling om tijdig bij te kunnen sturen in het proces. Daarnaast is de actualiteit met de komst van nieuwe statussen in BAG 2.0 ook verbeterd. Het resultaat van deze aanpassingen zal in de volgende zelfevaluatie inzichtelijk zijn.</i></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. 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>Gemeenten zijn samen met andere overheidsorganisaties bronhouder voor deze basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BRO. Omdat Goirle nog niet actief gestart is met het zelf bijhouden van de BRO hoeft er voor 2020 nog geen verantwoording te worden afgelegd.</p> <p>In 2021 start Goirle in samenwerking met Hilvarenbeek en Oisterwijk met de implementatie van de BRO.</p>	