College

Raadsinformatiebrief

Aan	Raad
Portefeuillehouder	Mark van Stappershoef
Onderwerp	Stand van zaken informatiebeveiliging en privacy 2019
Datum	14-05-2020

Kennisnemen van
deze raadsinformatiebrief waarmee we inzicht geven in, en verantwoording afleggen over de stand van zaken op het gebied van informatieveiligheid en privacy binnen onze organisatie.

Inleiding
In deze raadsinformatiebrief informeren wij u over de stand van zaken op het gebied van informatieveiligheid, de Algemene Verordening Gegevensbescherming (hierna: AVG) en de Eenduidige Normatiek Single Information Audit (hierna: ENSIA). We gaan in op de gevolgen hiervan voor Goirle en hoe dit in onze gemeente is geïmplementeerd.

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

ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid te professionaliseren door het toezicht te bundelen. ENSIA sluit aan op de gemeentelijke planning en control cyclus voor informatiebeveiliging, neemt de landelijke Baseline Informatiebeveiliging Gemeenten (BIG) 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.
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).

Vervolg
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 (reisdocumenten)
- Basisregistratie Grootschalige 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.

Logius levert diensten aan overheidsorganisaties en organisaties met een publieke taak. Voorbeelden van diensten zijn DigiD, Digipoort, MijnOverheid en eHerkenning.
Het Bureau Keteninformatisering Werk & Inkomen (BKWI) is een zelfstandig organisatieonderdeel binnen het UWV en vormt de schakel tussen ketenpartners op het gebied van werk en inkomen, zoals het UWV, de gemeenten en de SVB. Het BKWI adviseert en beheert met name ketenproducten zoals SUWInet.

Uit de verschillende zelfevaluaties en de externe audit blijkt dat gemeente Goirle informatiebeveiliging over het geheel gezien goed heeft geborgd. Er zijn verbeterpunten die opgepakt worden en waarbij de voortgang bewaakt wordt. Voor de Basisregistratie Ondergrond (BRO) voldoen we nog niet aan de gestelde norm. Alle verbeterpunten worden herleidbaar opgenomen in een plan van aanpak voor de implementatie van de BRO.

ENSIA verantwoording

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 per onderdeel weergegeven. Per onderdeel zijn ook de bevindingen kort uitgewerkt ter onderbouwing van deze status.

Legenda:

		
Ruim voldoende tot goed	***Voldoende***	***Onvoldoende***
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.

Verantwoording over de Baseline Informatiebeveiliging Gemeenten (BIG)
Tabel 1 geeft per BIG onderdeel een korte toelichting van de stand van zaken.

Baseline onderdeel	**Stand van zaken**	**Status**
BELEID EN ORGANISATIE Actueel beleid en organisatie van informatie-beveiliging, controle op naleving	Wat hebben we bereikt? Allereerst hebben we in GHO verband een team informatieveiligheid en privacy geformeerd dat sinds eind 2018 actief is. Dit team wordt gevormd door de CISO, ENSIA-coördinator, FG en twee privacy officers. In februari is GHO-breed beleid m.b.t. informatieveiligheid en privacy vastgesteld. In 2019 hebben we veel aandacht besteed aan bewustwording in de organisatie. **Beleid** In 2013 hebben alle gemeenten zich gecommitteerd aan de BIG als normenkader voor de informatiebeveiliging. In 2020 wordt de BIG vervangen door de BIO (Baseline Informatieveiligheid Overheid) als normenkader voor informatiebeveiliging binnen de gehele overheid. In voorbereiding daarop is in 2019 het beleid geactualiseerd. In februari is GHO-breed het strategisch beleid informatieveiligheid en privacy 2019-2021 vastgesteld. Dit is een drietraps model.	

	Het strategisch beleid is een beleidsstuk op hoofdlijnen. Hieronder ligt een tactisch kader dat is gemandateerd aan de directie, waarin de technische en organisatorische maatregelen, die de BIO en AVG vereisen, verder zijn uitgewerkt. De derde laag bestaat uit procedures en werkafspraken op afdelingsniveau die aanvullend nog nodig zijn. **Informatieveiligheid en ENSIA** De focus van de BIO ligt op een risico gestuurde aanpak. Er is in 2019 een begin gemaakt met het opzetten van een kwaliteitssysteem (PDCA cyclus) voor informatieveiligheid en privacy. De verantwoording over onze informatieveiligheid vindt plaats via ENSIA. Met het opzetten van dit kwaliteitssysteem zijn we voorbereid op de omslag van ENSIA van BIG naar BIO als leidend kader. In 2019 is met ENSIA nog verantwoording afgelegd op basis van de BIG. **Bewustwording** Voor de beleidsperiode 2019-2021 ligt de focus van het team IV&P op bewustwording. Er is daarom een awareness plan 2019-2021 opgesteld. Het grootste risico voor onze informatieveiligheid ligt volgens onderzoek van de VNG bij de mens. In dit kader investeren we in onze 'human firewall'. In 2019 hebben we GHO-breed 24 workshops over de AVG en informatieveiligheid gegeven. We maken gebruik van de mogelijkheden die ons gezamenlijke intranet ons biedt in een eigen themapagina. We hebben geborgd dat ook nieuwe medewerkers tijdig worden bijgepraat over Informatieveiligheid en Privacy. In Goirle en Hilvarenbeek is dit een onderdeel van de introductiedag, in Oisterwijk krijgen nieuwe medewerkers een aparte uitnodiging voor deze workshop, die een aantal keer per jaar zal worden gegeven. En er is een E-learning aangeboden over informatieveiligheid. **Privacy** In 2019 hebben we de basis voor alle privacy werkzaamheden verder op orde gebracht. In Goirle is het verwerkingsregister afgerond. In Hilvarenbeek en Oisterwijk is gestart met projecten voor een geheel nieuw verwerkingsregister. Hier is voor gekozen omdat deze registers niet alleen wettelijk verplicht zijn, maar ook als basis dienen voor andere werkzaamheden van ons team. Een goede, duidelijke en actuele basis is dan ook essentieel. Privacy is geborgd in tal van processen waaronder inkoop (bij alle inkoop vanaf 25.000 euro). Tot slot hebben 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.	
PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	**Fysieke toegang** Binnen GHO is de beveiliging van de panden technisch op orde. Er is zonering aanwezig, met de verdeling tussen publiek toegankelijke zones en gebieden waar alleen medewerkers mogen komen (doelbinding). Daarnaast zijn er ruimtes met specifieke doelbinding, zoals de ruimten van burgerzaken, of de serverruimten. Het instroom- doorstroom- en uitstroom proces is op orde en er is beheer op sleutels en toegangsbadges. Ondanks bovenstaande zijn er in de risicoanalyse een aantal risico's gebleken (zoals toegang tot de werkruimte van Burgerzaken). Deze zijn in de PDCA cyclus benoemd en mitigerende maatregelen worden door de proceseigenaren opgepakt. In algemene zin geldt dat de processen in opzet en bestaan aanwezig zijn, maar dat in de werking meer sturing en bijhouding nodig is. De veiligheidsnorm voor de overheid (BIO) vereist dat uitgegeven toegangsrechten (sleutels maar ook toegang tot systemen) twee tot vier keer per jaar worden gecontroleerd. Dat is nu (nog) niet altijd het geval. **Toegang tot systemen** Dit vindt plaats in samenwerking met Equalit. Volgens de norm wordt hiervoor een autorisatiematrix gehanteerd, waarbij goed wordt gekeken wie waartoe toegang mag krijgen. Sinds de komst van de AVG wordt hier een strengere lijn in gehanteerd, waarbij doelbinding van belang is. Toegang tot het netwerk vindt (buiten het pand) altijd plaats met tweefactor authenticatie. Er wordt nagedacht om dit ook binnen de panden toe te passen, omdat alleen een inlognaam en wachtwoord in deze tijd niet meer als afdoende veilig wordt gezien.	☺
CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienst-verlening en opvolging van incidenten	De continuïteit van onze dienstverlening is van cruciaal belang. Als we geconfronteerd worden met een incident of calamiteit moet hierop adequaat en gedegen gereageerd worden. Wat ons ook overkomt, de dienstverlening moet binnen afgesproken (en soms wettelijke) termijnen weer operationeel zijn. Dit vraagt om een goede borging van bedrijfscontinuïteitmanagement. Onze ICT systemen zijn ingericht dat calamiteiten kunnen worden opgevangen. Echter testen we niet periodiek of de getroffen maatregelen voldoende zijn om na zo'n calamiteit onze kritische bedrijfsprocessen weer operationeel te krijgen.	☺

	Incidenten komen ook bij ons regelmatig voor. Vaak zijn dit kleine zaken die eenvoudig worden opgelost. Afgelopen jaar waren er enkele grotere incidenten. Leerpunten hieruit worden meegenomen in het continue verbeteren van processen en afspraken.	
INFORMATIE-SYSTEMEN Veilige omgang met informatiesys-temen en afspraken hierover met onze leveranciers	Het beheer van ICT bedrijfsmiddelen is goed georganiseerd in samenwerking met Equalit. Hard- en software is zoveel mogelijk centraal in beeld en in beheer. Echter er vindt ook door de gemeente zelf aanschaf en beheer van mobile devices plaats, zoals bijvoorbeeld telefoons of tablets. Met Equalit zijn goede afspraken gemaakt om scheiding van informatie veilig op deze apparaten te regelen (Mobile Device Management). Binnen de informatiesystemen zullen autorisaties strakker moeten worden ingezet. Het aanscherpen van functiescheiding binnen de processen en onderliggende voorzieningen is nodig. Beveiligde gegevensuitwisseling voor communicatie met inwoners en (keten)partners wordt in 2020 ingericht, in lijn met de nieuwe norm vanuit de zorg: de NTA7516. Maar een veilige uitwisseling van gegevens wordt ook vanuit onze eigen norm, de BIO, vereist en geldt voor alle bedrijfsgegevens, in het bijzonder die waar persoonsgegevens worden uitgewisseld. We kiezen er daarom voor om, in samenwerking met Equalit, een organisatie brede oplossing voor veilig mailen aan te schaffen.	☺
DATABESCHER-MING Veilige omgang met data in onze software	Dataclassificatie is noodzakelijk in het kader van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie gaat over de mate van gevoeligheid en bescherming. "De juiste informatie op het juiste moment bij de juiste persoon". Binnen de basisregistraties en het digitaal loket (website) is dataclassificatie op orde. Dit is echter nog niet voor alle informatiesystemen geregeld.	☺

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**
Suwinet Structuur uitvoerings-organisatie Werk en Inkomen	Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet en adresonderzoeken (ter verbetering van de Basis Registratie Personen). 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 Goirle 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. DigiD 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. Het onderzoek van de externe auditor geeft aan dat onze processen rondom DigiD goed op orde zijn. Ons digitale loketten (Brein en WOZ-loket) voldoen aan de gestelde informatiebeveiligingsnormen en het beheer hiervan is op orde.	☺
BRP Basis Registratie Personen	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.	☺

	De zelfevaluatie BRP over het jaar 2019 is met een heel mooi resultaat afgerond met • 99,18 % op de kwaliteit van de persoonsgegevens • 97,8 % op de kwaliteit van de processen De gemeente scoort hiermee ruim boven de landelijk gestelde norm.	
PUN Paspoort Uitvoerings-regeling 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. 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 informeren we ook het eigen bestuur over de stand van zaken. De zelfevaluatie PUN 2019 is afgerond met een score van 96,6 %. 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.	☺
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 2019 is afgerond met een prachtige score van 150 van maximaal 150. Hiermee voldoen we helemaal aan de landelijk gestelde norm van 113. Ondanks dat we 100% hebben gescoord, is er toch een verbeterpunt te benoemen. Alle processen zijn vastgelegd, maar deze zijn nog niet samengebracht in één processenhandboek. In 2020 worden daarom de verschillende (reeds vastgelegde) processen gebundeld tot één BGT-processenhandboek.”	☺
BAG Basisregistratie Adressen en	De BAG bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Kopieën van al deze gegevens zijn verzameld in een landelijke voorziening. Deze voorziening wordt landelijk gebruikt door overheden, organisaties en particulieren. Net als alle andere bronhouders	☺

Gebouwen	verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BAG. De zelfevaluatie BAG over het jaar 2019 is afgerond met een score van 170 van maximaal 205. Hiermee voldoen we goed aan de landelijk gestelde norm van 154. De verbeterpunten worden opgenomen in een plan van aanpak. In 2020 zal de nodige inspanning geleverd worden om de BAG en WOZ verder op elkaar af te stemmen m.b.t. gebruiksoppervlakte en bouwjaren. Hiervoor zal de nodige capaciteit vrij gemaakt moeten worden.	
BRO Basisregistratie Ondergrond	De BRO bevat bodem- en ondergrondgegevens. 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. Het aanstellen van een BRO-coördinator heeft de hoogste prioriteit. Intern is er geen capaciteit beschikbaar. Om deze reden zal in 2020 in GHO-verband (Goirle – Hilvarenbeek – Oisterwijk) gekeken worden om deze functie in te vullen. Daarnaast moet ook een vervanger aangesteld worden.	☹