College

Raadsinformatiebrief

Aan	Raad
Portefeuillehouder	Mark van Stappershoef
Onderwerp	Raadsinformatiebrief Informatiebeveiliging en privacy
Datum	01-05-2019

Kennisnemen van
De BIG, AVG en ENSIA

Inleiding
In deze raadsinformatiebrief informeren wij u over de Baseline informatiebeveiliging Nederlandse gemeenten (hierna: BIG), 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
Wat is de Baseline informatiebeveiliging Nederlandse Gemeenten (BIG)?
De VNG heeft de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Deze resolutie moet zorgen voor een verbetering van de informatieveiligheid door de implementatie van de BIG. De BIG bevat ruim 300 richtlijnen en voorschriften die bij naleving zorgen voor een acceptabel niveau van informatiebeveiliging binnen de gemeente. De BIG is opgezet rondom bestaande normen zoals de Algemene Verordening Gegevensbescherming, de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen, de Basisregistratie Personen, de Basisregistratie Adressen en Gebouwen en de Wet Paspoortuitvoeringsregeling.

Wat is de Algemene Verordening Gegevensbescherming (AVG)?
Sinds 25 mei 2018 moeten we ons aan de AVG houden. Deze wetgeving moet ervoor zorgen dat de huidige privacyregelgeving in Europa op een gelijke manier wordt geregeld. Daarnaast zorgt de AVG voor een verbetering van de privacy (bescherming) van burgers. Gemeenten hebben een grote verantwoordelijkheid waar het gaat om de omgang met persoonsgegevens. En daarom moeten we op een juiste en veilige manier omgaan met de persoonsgegevens van onze burgers.

Wat is ENSIA (Eenduidige Normatiek Single Information Audit)?
ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke planning- en control-cyclus. De BIG is de kern van de verantwoording over informatieveiligheid aan de gemeenteraad. Deze verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het college van B&W en een passage over informatieveiligheid in het jaarverslag aan de raad.

Wat betekent dit voor Goirle?

Activiteiten in 2018 met betrekking tot Informatieveiligheid en Privacy

- Er is in 2018 een GHO-breed (Goirle, Hilvarenbeek en Oisterwijk) virtueel team ingericht dat zorg draagt voor een permanente borging van privacy en informatieveiligheid in de organisatie. Dit team bestaat uit de Functionaris Gegevensbescherming (FG), die als onafhankelijk toezichthouder fungeert op de naleving van de privacywetgeving , twee Privacy Officers (PO) die de FG ondersteunen, een Chief Information Security Officer (CISO) die verantwoordelijk is voor de informatieveiligheid en een ENSIA coördinator (meer over ENSIA hieronder).
- Gestart is met het opstellen van het strategisch beleid Informatieveiligheid en Privacy, omdat het bestaande beleid in 2018 afliep. Hierin zijn de onderdelen veiligheid en privacy integraal verwerkt. Gekozen is voor een aanpak op strategisch, tactisch en operationeel niveau, waarbij aansluiting wordt gezocht op de BIO (Baseline Informatievoorziening Overheid), die in 2020 in werking zal treden. Tevens is ervoor gekozen het beleidsplan voor GHO te harmoniseren en door de drie colleges te laten vaststellen.
- Met ENSIA (Eenduidige Normatiek Single Information Audit) leggen gemeenten in één keer verantwoording af over informatieveiligheid gebaseerd op de BIG (Baseline Informatie-beveiliging Nederlandse Gemeenten). Hiermee wordt de verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) samengevoegd en gestroomlijnd. In december 2018 hebben we deze onderzoeken uitgevoerd. Het college legt met een collegeverklaring verantwoording af over DigiD en Suwinet. Hierover is in maart 2019 door een externe auditor assurance gegeven. Met de managementrapportages wordt over de BRP, PUN, BAG, BGT en BRO verantwoording afgelegd aan de verticale toezichthouders (de verschillende ministeries). Dit jaar is voor de BRO nog een pilot.

Verantwoording per onderdeel ENSIA

Onderstaande tabel geeft per (ENSIA) onderdeel een korte toelichting, bevindingen en de stand van zaken weer.

Domein Onderdeel	**Bevindingen & verbeteracties**	**Status**
Basis Registratie Personen (BRP)	De zelfevaluatie BRP over het jaar 2018 is met een heel mooi resultaat afgerond met 99,23 % op de kwaliteit van de persoonsgegevens en 99.1 % op de kwaliteit van de processen. Voor de BRP is gemeente Goirle geselecteerd voor een landelijke steekproef.	
Paspoort Uitvoeringsregeling Nederland (PUN)	De zelfevaluatie PUN over het jaar 2018 is afgerond met een score van 97,9 %. Eindresultaat is het oordeel dat gemeente Goirle de Paspoort Uitvoeringsregeling Nederland goed uitvoert. Voor de PUN is gemeente Goirle niet geselecteerd voor een steekproef.	
Digitale Persoons-identificatie (DigiD)	Het onderzoek van de externe auditor over DigiD geeft aan dat we goed scoren. Onze digitale loketten (Brein en WOZ-loket) voldoen aan de informatie-beveiligingsnormen en het beheer is op orde.	
Basisregistratie Grootschalige Topografie (BGT)	De zelfevaluatie BGT over het jaar 2018 is afgerond met een score van 150 van maximaal 150 (100%). Hiermee is ruim voldaan aan de landelijk gewenste minimale norm van 120 (75%). Een heel mooie score.	
Basisregistratie Adressen en Gebouwen (BAG)	De zelfevaluatie BAG over het jaar 2018 is afgerond met een score van 195 van maximaal 205 punten (95%). Ook een heel mooi resultaat.	
Basisregistratie Ondergrond (BRO)	De zelfevaluatie BRO was dit jaar nog niet verplicht maar is gebruikt als Nulmeting. In deze eerste zelfevaluatie scoort onze gemeente 0 van de maximaal 120 punten (0,0 %). In 2019 zal een BRO-coördinator aangesteld moeten worden die vervolgens een plan van aanpak gaat opstellen om de BRO te implementeren.	
Structuur Uitvoeringsorga-nisatie Werk en Inkomen (Suwinet)	Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet en voor het uitvoeren van adresonderzoeken (ter verbetering van de Basis Registratie Personen). Uit de zelfevaluatie blijkt dat de gemeente goed scoort in het kader van informatieveiligheid rondom het gebruik en beheer van Suwinet.	

AVG

- Medewerkers hebben voorlichting gehad over de nieuwe privacywetgeving, de Algemene Verordening Gegevensbescherming (AVG). Hiervoor is zowel gebruik gemaakt van workshops (gegeven door de functionaris gegevensbescherming en de privacy officer) als door het aanbieden van een E-learning op dit gebied.

- In 2019 organiseren we per afdeling nieuwe workshops om kennis en bewustwording binnen de organisatie verder te vergroten.
- Er is een register van verwerkingen opgesteld. Het maken en beheren van dit register is een nieuwe verplichting die de AVG met zich meebrengt.
- Er zijn procedures ingericht voor alle (deels nieuwe) rechten die betrokkenen hebben onder de AVG.
- Er is een gemeentelijke verwerkersovereenkomst opgesteld, waarin duidelijke afspraken worden gemaakt over het verwerken van persoonsgegevens door derde partijen. Met vrijwel alle partijen met wie we als gemeente gegevens delen is inmiddels ook een verwerkers-overeenkomst gesloten.
- Bestaande werkwijzen en procedures zijn deels beoordeeld in het licht van de privacyregels en waar nodig aangepast. Dit gebeurt nu nog zowel op initiatief van de medewerkers zelf als op initiatief van Functionaris Gegevensbescherming/Privacy Officer, maar zal in 2019 (en daarna) steeds meer volgens een planmatige aanpak gaan gebeuren.
- Beveiligd e-mailen is ingevoerd, door middel van de tool Sharefile.

Vervolg
Omdat in 2020 de BIO (Baseline Informatieveiligheid Overheid) in werking treedt starten we in 2019 met de implementatie hiervan. Daarbij zijn de volgende items speerpunten: bewustwording, organisatiebrede governance (taken, bevoegdheden en verantwoordelijkheden op het gebied van informatieveiligheid) en een integrale verantwoording.

Communicatie
We organiseren een informatiebijeenkomst voor de raden van de GHO-gemeenten.
Daar vertellen we over het toezicht op informatieveiligheid en willen we de urgentie hiervoor benoemen. Het strategisch beleid informatieveiligheid en privacy staat op de websites van de GHO-gemeenten.