Raadsinformatiebrief

Aan:	Leden van de raad
Van:	College van burgemeester en wethouders
Datum:	22 mei 2018
Onderwerp:	Stand van zaken informatiebeveiliging en privacy
Doel:	Ter kennisname/ ter informatie
Aanleiding:	Informatie (algemeen)
Aard informatie:	Openbaar

Aanleiding
Op 23 januari informeerden wij u over de Baseline informatiebeveiliging Nederlandse gemeenten (hierna: BIG), de Algemene Verordening Gegevensbescherming (hierna: AVG), de Wet datalekken en de Eenduidige Normatiek Single Information Audit (ENSIA), de gevolgen hiervan voor Heusden en de wijze waarop een en ander in onze gemeente wordt geïmplementeerd. Voor de volledigheid is de raadsinformatiebrief van 23 januari als bijlage bij deze informatiebrief opgenomen.

In deze raadsinformatiebrief leest u de stand van zaken over de invoering van de AVG en BIG.

Informatie
Hoe privacyproof zijn wij op 25 mei?
Op 25 mei 2018 moeten we tenminste aan zes verplichte AVG-maatregelen voldoen. Deze treft u hieronder aan inclusief de stand van zaken in Heusden.

1. Heusden moet beschikken over een register van verwerkingsactiviteiten.
   De 60 meest kritische verwerkingsprocessen zijn volledig in kaart gebracht. De overige verwerkingsprocessen zijn in concept in kaart gebracht en worden na 25 mei 2018 verder opgepakt

2. Heusden moet een data privacy impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico kunnen uitvoeren.
   Onze Chief Informationsecurity Officer, Functionaris Gegevensbescherming en vakspecialisten voeren impactanalyses uit bij de aanschaf van een nieuwe applicatie of verwerking zoals digitaliseren van de personeelsdossiers.

3. Heusden moet beschikken over van een register van datalekken die zijn opgetreden en een datalekprotocol.
   We beschikken over een datalekregister en een protocol.

4. Heusden moet kunnen aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer daarvoor toestemming nodig is.
   Hierbij hanteren we een omgekeerde werkwijze: door middel van een privacyverklaring op onze website informeren we de klant hoe we omgaan met persoonsgegevens en wat de rechten van de klant zijn. Over het algemeen is het overigens zo dat de gemeente een wettelijke grondslag heeft voor de verwerking van persoonsgegevens en handelt in het kader van algemeen belang. Daarbij is een expliciete toestemming van de klant niet nodig. Wel vinden wij het van belang de klanten goed te informeren over de verwerking van persoonsgegevens.

5. Heusden moet een Functionaris gegevensbescherming hebben aangesteld en aangemeld bij de Autoriteit persoonsgegevens;

We beschikken nu over een Functionaris Gegevensbescherming die tijdelijk is aangesteld en aangemeld. Er wordt nog geëvalueerd hoe dit definitief in de organisatie kan worden ingebed.

6. Heusden moet beschikken over een procedure voor inzage in persoonsgegevens.
   Deze procedure wordt naar verwachting op 23 mei 2018 in het managementteam vastgesteld.

   Naast deze 6 verplichte AVG-maatregelen hebben we op 20 maart 2018 het privacybeleid en privacyreglement voor Heusden vastgesteld. Doel van het privacybeleid en -reglement is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente persoonsgegevens verwerkt. Tenslotte wordt er momenteel gewerkt aan 36 verwerkersovereenkomsten. Dit zijn overeenkomsten met externe partijen die persoonsgegevens voor ons verwerken. In deze overeenkomsten worden afspraken gemaakt over de verwerking en de verantwoordelijkheden om zo risico's tot een minimum te beperken.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacywetgeving. Zo kan de AP uit eigen beweging een onderzoek doen naar de naleving van de privacywetgeving. Dit heet ambtshalve onderzoek. De AP kan zo'n onderzoek bijvoorbeeld starten vanwege actuele gebeurtenissen of tips die de AP ontvangt over mogelijke overtredingen van de wet. Daarnaast kan de AP op verzoek van belanghebbenden (zoals burgers of belangenorganisaties) een onderzoek instellen. Met de maatregelen die we tot nu toe hebben genomen zijn we goed voorbereid op een dergelijk onderzoek.
Overigens is de verwachting dat de AP na 25 mei 2018 in het algemeen niet direct tot het opleggen van boetes overgaat maar aanwijzingen zal geven als een situatie daar aanleiding toe geeft.

Hoe verloopt de implementatie van de BIG?
In overleg met de accountant is besloten om in 2018 te werken aan 4 prioriteiten. Deze treft u hieronder aan inclusief de stand van zaken.

1. <u>De organisatie van de informatiebeveiliging en bewustwording</u>
   Informatiebeveiliging gaat niet enkel over de 'harde' kant zoals virusscanners en wachtwoorden. Zeker ook het menselijk handelen bepaalt hoe veilig er wordt omgegaan met (gemeentelijke) informatie. In de afgelopen maanden is veel energie gestoken in bewustwordingsacties onder alle medewerkers door middel van een lezing, interne nieuwsbrief, ludieke phishing mail en gesprekken met alle clusters in onze organisatie. Medewerkers hebben zo kennis opgebouwd wat resulteert in een alerte houding ten aanzien van beveiligingsrisico's. Medewerkers zijn daardoor in staat om juiste beslissingen te nemen in de omgang met gevoelige informatie.

2. <u>Bedrijfscontinuïteit</u>
   Met betrekking tot bedrijfscontinuïteit zijn de meest kritische bedrijfsprocessen in beeld gebracht. Een volgende stap is nu om ervoor te zorgen dat onderbrekingen van deze kritische processen worden tegengegaan en worden beschermd tegen de gevolgen van onderbrekingen.

3. <u>Verwerving, onderhoud en ontwikkeling van systemen</u>
   Het is van belang dat beveiliging wordt ingebouwd in bestaande en nieuwe informatiesystemen. Hiervoor wordt het beveiligingsniveau van bestaande systemen in beeld gebracht en vertaald naar beheersmaatregelen. Op dit moment is de Chief Informationsecurity Officer vooral betrokken bij de aanschaf van nieuwe systemen en de beveiliging van deze systemen. Er moet nog worden onderzocht hoe beveiliging en privacy integraal onderdeel kunnen worden in aanbestedingen en hoe beveiligingsrisicoanalyses kunnen worden geborgd bij projecten. Daarnaast worden bestaande informatiesystemen nog tegen het licht gehouden.

4. P&C-cyclus implementeren met een Information Security Management System (ISMS)
   Het bestuurlijk en organisatorisch borgen van informatieveiligheid door aansluiten bij de bestaande planning&control-cyclus is een must. Een zogenaamd ISMS-systeem helpt daarbij. Een ISMS-systeem zorgt ervoor dat beveiligingsrisico's in beeld zijn met daaraan gekoppeld maatregelen en planning. Daarnaast kunnen incidenten worden geregistreerd en maakt een ISMS het gemakkelijk om verantwoording af te leggen in het kader van de ENSIA. Er moet nog een oriëntatie plaatsvinden op welk ISMS-systeem voor Heusden geschikt is.

M E M O R A A D

Aan:	de leden van de raad
Van:	Het college van Heusden
Datum:	23 januari 2018
Onderwerp:	Informatiebeveiliging en privacy
Doel:	ter kennisname/ter informatie
Aanleiding:	informatie (algemeen)
Aard informatie:	openbaar

Aanleiding / voorgeschiedenis
In dit memo wordt u geïnformeerd over de Baseline informatiebeveiliging Nederlandse gemeenten (hierna: BIG), de Algemene Verordening Gegevensbescherming (hierna: AVG), de Wet datalekken en de Eenduidige Normatiek Single Information Audit (ENSIA). Er wordt ingegaan op de gevolgen hiervan voor Heusden en hoe dit in onze gemeente wordt 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 Wet bescherming persoonsgegevens, de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen, de Gemeentelijke Basisadministratie, de Basisregistratie Adressen en Gebouwen en de Wet Paspoortuitvoeringsregeling.

Wat is de Algemene Verordening Gegevensbescherming (AVG)?
Op 25 mei 2016 is de AVG in werking getreden. Deze nieuwe wetgeving moet zorgen voor harmonisatie van de huidige privacyregelgeving in Europa en verbetering van de privacy(bescherming) van burgers. Gemeenten hebben een grote verantwoordelijkheid waar het gaat om de omgang met persoonsgegevens. Om gemeenten te ondersteunen bij de implementatie van de AVG is door de VNG onder meer het Raamwerk Privacy en de, hiervoor genoemde, BIG ontwikkeld. Het Raamwerk Privacy en de BIG helpt gemeenten om privacy goed te borgen. Gemeenten hebben tot 25 mei 2018 de tijd om aan de AVG te voldoen.

Wat is de Wet Datalekken?
Alle bedrijven en overheden die persoonsgegevens verwerken op grond van de Wet bescherming persoonsgegevens (Wbp) zijn vanaf 1 januari 2016 verplicht om een ernstig datalek direct te melden aan de Autoriteit Persoonsgegevens. Of een datalek gemeld moet worden is afhankelijk van de (potentiële) impact van het datalek op de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. Onder een datalek valt het vrijkomen (lekken) van persoonsgegevens, maar ook vernietiging daarvan en andere vormen van onrechtmatige verwerking. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand. De autoriteit Persoonsgegevens kan bij een ernstig datalek een boete opleggen. Deze boete kan oplopen tot € 820.000.

Onze gemeente heeft tot nu toe twee officiële meldingen gedaan op grond van de Wet datalekken die niet hebben geleid tot een boete. Mocht er in de toekomst sprake zijn van een datalek dan moeten we kunnen aantonen dat we de nodige maatregelen uit de BIG en AVG hebben getroffen om de kans op een datalek zo klein mogelijk te maken.

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. De ENSIA komt in de plaats van de huidige verantwoording op het gebied van DigiD en Suwi (Structuur Werk en Inkomen) en wordt in 2018 verder uitgebreid om uiteindelijk alle normen uit de BIG, BRP (basisregistratie personen), PUN (paspoort uitvoeringsregeling Nederland), BAG (basisregistratie adressen en gebouwen), BGT (basisregistratie grootschalige topografie) te bestrijken.

Wat betekent dit voor Heusden?
Informatiebeveiliging en privacy zijn erg actueel. Regelmatig verschijnen berichten over gehackte systemen en datalekken in de media. In het kader van onze begroting heeft u vragen gesteld over de stand van zaken over informatiebeveiliging en privacy. In de begroting voor 2018 is in de bedrijfsvoeringparagraaf aangekondigd dat Heusden op het gebied van informatiebeveiliging en privacy nog onvoldoende scoort en dat een verbetertraject noodzakelijk is om de informatiebeveiliging en gegevensbescherming op een adequaat niveau te krijgen. Daarnaast worden we op korte termijn op het gebied van de AVG en ENSIA geconfronteerd met wettelijke deadlines. Heusden is nog kwetsbaar op dit gebied en is daarom eind 2017 hiermee aan de slag gegaan. Belangrijkste focus is daarbij bewustwording en in control komen.

In samenwerking met een extern bureau (IvO-partners) wordt, op basis van een analyse, de implementatie opgepakt**.** De analyse laat zien dat een inhaalslag noodzakelijk is om op het gebied van informatiebeveiliging en privacy op een adequaat niveau te komen. Daarbij is het streven om zo veilig mogelijk te werken en afgewogen risico's te accepteren. Dit houdt in dat er wordt gekozen voor een praktische insteek met een juiste balans tussen veiligheid en een werkbare situatie.

Hieronder worden de acties die voor de implementatie nodig zijn, per onderdeel, kort toegelicht.

Project BIG
Aan de hand van een analyse is het verschil tussen de bestaande en de gewenste situatie op het gebied van informatiebeveiliging, in beeld gebracht. Deze analyse brengt de risico's op het gebied van informatiebeveiliging in beeld. In afstemming met de accountant wordt in 2018 gewerkt aan de volgende 4 prioriteiten:

- de organisatie van de informatiebeveiliging en bewustwording;
- bedrijfscontinuïteit;
- verwerving, onderhoud en ontwikkeling van systemen;
- implementatie van informatiebeveiliging en maatregelen in de planning- en controlcyclus.

Met de overige onderdelen uit de BIG wordt in 2018 een start gemaakt waarna dit in 2019 een vervolg krijgt. De verwachting is dat hiermee voldoende inspanning wordt geleverd om BIG-proof te worden.

Het beoogde resultaat van het project BIG is meer grip hebben op informatieveiligheid waarbij risico's zijn afgewogen, waar nodig maatregelen zijn getroffen en informatieveiligheid is ingebed in de organisatie.

Project AVG
Het project AVG gaat over de bescherming van privacygevoelige gegevens.
Het beoogde resultaat van het project AVG is om per 25 mei 2018 te voldoen aan de wettelijke verplichtingen van de AVG. Hiervoor worden, onder andere, de volgende acties ondernomen:

- bewustwording en kennisvergroting bij medewerkers die werken met privacygevoelige gegevens;
- registratie van de verwerkingen persoonsgegevens bij de Autoriteit Persoonsgegevens;
- borgen van de rechten van betrokkenen (inwoners) in de huidige procedures;
- inventarisatie van privacyrisico's in kritische bedrijfsprocessen en treffen van eventuele aanvullende maatregelen;
- informatiebeveiliging meenemen bij ontwerp en aanschaf van ICT-systemen;
- protocollen m.b.t. Meldplicht datalekken en bewerkersovereenkomsten vervaardigen;
- implementeren van de verantwoordingsplicht in de gemeentelijke PDCA-cyclus.

Voor het uitvoeren van dit project wordt tot juni 2018 een privacydeskundige in de rol van kwartiermaker ingehuurd die tijdens het project zijn kennis overdraagt aan de interne Functionaris Gegevensbescherming.

Project ENSIA

Het beoogde resultaat van het project ENSIA is het uitvoeren van de verplichte verantwoording aan de raad en landelijke toezichthouders voor 1 mei 2018 en de borging van informatiebeveiliging en de verantwoordingsplicht in de gemeentelijke PDCA-cyclus voor 2019. Dit doen we door het organiseren van het nieuwe verantwoordingsproces, het creëren van brede betrokkenheid in de organisatie en het vormgeven van de verantwoording over informatieveiligheid. Daarbij ligt het accent in de verantwoording over 2017 op DigiD en Suwi (wettelijk verplicht). In 2018 wordt dit verder uitgebreid naar andere terreinen.

De verantwoording in het kader van ENSIA ziet er stapsgewijs als volgt uit:

1. Uitvoering zelfevaluatie (vóór 31 december 2017)

Met een zelfevaluatie stelt het college vast of de informatiebeveiliging aan de normen[1] voldoet. De uitkomsten van de zelfevaluatie worden gerapporteerd aan ENSIA-autoriteit. Verbeterpunten uit deze zelfevaluatie worden meegenomen in de aanpak van informatiebeveiliging in 2018.

2. Verantwoording aan de raad (vóór 15 juli 2018)

Het college legt verantwoording af over informatiebeveiliging aan de raad in een paragraaf informatieveiligheid in het jaarverslag. Na vaststelling door de gemeenteraad vindt rapportage plaats aan het Ministerie van Binnenlandse zaken en Koninkrijksrelaties.

3. Verantwoording aan landelijke toezichthouders (vóór 1 mei 2018)

Voor 1 mei wordt gerapporteerd aan de landelijke toezichthouder. Belangrijk hierbij is dat in het jaarverslag een collegeverklaring informatieveiligheid is opgenomen en dat de auditor 'assurance' heeft gegeven over Suwi en DigiD.

Bij de afronding van het ENSIA-project zal een evaluatie worden uitgevoerd over de aanpak van de verantwoordingstraject. De ENSIA-verantwoording wordt voor eind 2018 geborgd in de staande organisatie.

[1] BIG-normen en specifieke normen voor de BRP, PUN, DigiD, SUWInet, BAG en BGT.

Inzet van middelen

	Eenmalige kosten 2018	Kosten 2019 en verder
Inhuur	79.400	
Kwartiermaker	42.000	
ENSIA	6.000	12.500
ISMS-systeem	20.000	2.500
Communicatie	3.500	
Totaal	**150.900**	**15.000**

De totale projectkosten bedragen voor 2018 € 150.900. De kosten van project ENSIA kunnen in 2018 worden gedekt uit bestaande middelen. De overige kosten ad € 144.900 zullen in de eerste bestuursrapportage worden meegenomen. De structurele kosten vanaf 2019 bedragen € 15.000 (in geval een ISMS aangeschaft wordt). Deze middelen kunnen niet worden gedekt uit reguliere budgetten en zodoende zijn aanvullende middelen nodig. Deze structurele kosten worden tevens meegenomen in de eerste bestuursrapportage.

Risico's

De gemeente Heusden voldoet momenteel nog niet aan de normen die op het gebied van informatiebeveiliging en privacy gesteld worden. De kans op een datalek of een gehackt systeem laat zich moeilijk inschatten. Indien dit zich voordoet dan kan dit flinke gevolgen hebben. Denk daarbij aan financiële en emotionele schade voor inwoners op het moment dat hun (privacygevoelige) gegevens op straat komen te liggen, een boete van de Autoriteit Persoonsgegevens, imagoschade en problemen in de dienstverlening.

Samengevat

We hebben geconstateerd dat Heusden op het gebied van informatiebeveiliging en privacy een inhaalslag moet maken. Wij hechten eraan dat de gegevens van burgers bij ons in goede handen zijn. We hebben geen signalen dat dit nu extra gevaar loopt, echter de aangescherpte regelgeving vraagt verdere inspanning (en dus een inhaalslag) van onze zijde.
Bij de aanpak wordt van een realistisch en praktisch scenario uitgegaan met als doel te voldoen aan de AVG en het bereiken van een adequaat niveau op het gebied van de informatiebeveiliging. Minder doen vergroot naar onze mening het risico op een datalek in de toekomst met alle gevolgen van dien. Wij hebben dan ook besloten om in 2018 de implementatie van de BIG en AVG voortvarend verder op te pakken.