gemeente **Barneveld**

Zaaknr. 1101313

Collegevoorstel

Onderwerp:
Voorstel jaarverslag functionaris gegevensbescherming 2018

Gevraagde beslissing:

1. Het bijgevoegde Jaarverslag FG 2018 vast te stellen;
2. De memo en het Jaarverslag FG 2018 via rubriek B ter kennisname te doen toekomen aan de gemeenteraad;
3. Ter voldoening aan de verplichte registratie en publicatie het Jaarverslag FG 2018 op de website van de gemeente te plaatsen.

Raad
☑ Ter kennisname naar de raad
Nummer beleidsproduct:
☐ Op overzicht Bestaand beleid (website)

Datum: 7 februari 2019 Steller: S.M.M. Beekman

Afd: Team Juridische Zaken (B&D) Aantal bijlagen 2

Afd.hoofd: Portefeuillehouder A. v/d Burgwal gezien

Openbaarheid
Besluit (voorblad) openbaar: ◉ Ja ○ Nee, zie beslispunt :
Groentje openbaar: ◉ Ja ○ Nee, zie beslispunt :
Bijlagen openbaar: ◉ Ja ○ Nee, vermelden op bijlage

	Akkoord	Bespreken	Aantekeningen
Secretaris			
Burgemeester			
Wethouder A. de Kruijf			
Wethouder P.J.T. van Daalen			
Wethouder A.H. van de Burgwal			
Wethouder D. J. Dorrestijn-Taal			

Beslissing burgemeester en wethouders : 26 FEB. 2019

Conform advies.

Nummer op besluitenlijst: 9/02.

1. Inleiding
Op grond van de Europese Algemene Verordening Gegevensbescherming (AVG), die per 25 mei 2018 de Wet bescherming persoonsgegevens heeft vervangen, en het Privacybeleid brengt de Functionaris Gegevensbescherming (FG) jaarlijks voor 1 maart verslag uit aan de bestuursorganen. In het verslag is toegelicht hoe de Gemeente Barneveld de AVG heeft geïmplementeerd en omgaat met de persoonsgegevens van inwoners, bedrijven en instanties. Dit verslag bevat informatie over de verantwoording van de verschillende functionarissen, de werkzaamheden en bevindingen, aanbevelingen en de te ondernemen acties voor het volgende jaar.

2. Beoogd effect
De bestuursorganen van de gemeente en de inwoners worden geïnformeerd over de wijze waarop de Gemeente Barneveld de AVG heeft geïmplementeerd en omgaat met de persoonsgegevens van inwoners, bedrijven en instanties.

3. Argumenten
1.1. De rapportage geeft een goed inzicht in de implementatie van de AVG en over hoe de gemeente omgaat met persoonsgegevens
Het verslagjaar ziet op de periode van 1 januari tot en met 31 december 2018. In de verslagperiode is hard gewerkt om aan de verplichtingen van de AVG te voldoen. Zo zijn de volgende vereisten (nagenoeg) gerealiseerd:
- aanstelling Functionaris Gegevensbescherming;
- aanstelling Privacy Officer;
- een register van verwerkingen (90% gereed);
- een privacyverklaring (voor op de website);
- een overzicht van de verwerkersovereenkomsten, het afsluiten van vele nieuwe of geactualiseerde verwerkersovereenkomsten;
- een overzicht van de rechten van betrokkenen (voor op de website);
- het uitvoeren van Privacy Impact Assessments (50% gereed);
- een overzicht van de voorgekomen beveiligingsincidenten en datalekken;
- een Privacybeleid en;
- bewustwording van medewerkers (door verplicht gestelde workshops en berichten op intranet).

2.1. Conform het Privacybeleid wordt de gemeenteraad geïnformeerd
De AVG en het Privacybeleid van de Gemeente Barneveld schrijven voor dat de FG jaarlijks voor 1 maart verslag uitbrengt aan de bestuursorganen. Het onderhavige verslag wordt dan ook uitgebracht aan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad van Barneveld.

4. Publicatie van het jaarverslag op de website geeft openheid
Met het publiceren van het Jaarverslag FG 2018 voldoet het college aan de in de AVG en het Privacybeleid opgenomen verplichting. Hiermee geeft uw college aan de inwoners en andere belangstellenden opening van zaken over de implementatie van de AVG in de afgelopen periode van 1 januari tot en met 31 december 2018. In het verslagjaar wordt toegelicht welke werkzaamheden zijn uitgevoerd en wat de acties voor het komende jaar zijn.

4. Kanttekeningen
N.v.t.

5. Financiën
N.v.t.

6. Uitvoering
N.v.t.

7. Bijlagen
1. Jaarverslag FG 2018
2. Memo aan raad

gemeente Barneveld

Jaarverslag

Functionaris Gegevensbescherming 2018

Jaarverslag

Functionaris Gegevensbescherming 2018

Opdrachtgever:	gemeente Barneveld Afdeling Bestuur & Dienstverlening
Auteur:	Sascha Beekman, Functionaris Gegevensbescherming
Datum:	7 februari 2019

Inhoud

1. MANAGEMENTSAMENVATTING

Op 25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing geworden in de hele Europese Unie. In Nederland is op die dag de Wet bescherming Persoonsgegevens komen te vervallen.

De gemeente Barneveld heeft de bescherming van de privacy van de Barneveldse inwoners en het verwerken van de (persoons)gegevens van deze inwoners met de komst van de AVG opnieuw beoordeeld en waar nodig verbeterd. Zo is er in 2018 een Privacybeleid opgesteld en zijn de inwoners via de gemeentelijke website en door middel van informatiebijeenkomsten geïnformeerd over de AVG, hun rechten en hoe de Gemeente Barneveld de bescherming van de verwerking van de (persoons) gegevens waarborgt.

In dit jaarverslag – dat mede in samenwerking met de Privacy Officer (PO) en de Chief Information Security Officer (CISO) – door de Functionaris Gegevensbescherming (FG) is opgesteld, geeft weer wat de Gemeente Barneveld in 2018 heeft ondernomen om aan de vereisten van de AVG te voldoen. Behalve dat er een Privacybeleid is opgesteld, is er hard gewerkt aan het opstellen van een register van verwerkingen en zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met vele verwerkers. Ook zijn er intern veel adviezen gegeven en workshops gehouden over privacy en informatieveiligheid, omdat deze onlosmakelijk met elkaar verbonden zijn en het belangrijk is dat het bewustzijn bij de medewerkers aanwezig is en dat ook blijft. Daarbij is niet alleen aandacht besteed aan de grondslag en doelbinding die aanwezig moet zijn voordat gegevens verwerkt mogen worden, welke gegevens verwerkt mogen worden en hoe lang deze bewaard mogen worden, maar ook is het belang onderstreept van een zorgvuldige verwerking en deling van gegevens door bijvoorbeeld gebruik te maken van beveiligd e-mailen.

In 2018 is een begin gemaakt met het uitvoeren van Privacy Impact Assessments (PIA's), waarmee een goede risico-analyse gemaakt kan worden over hoe er per vakgebied omgegaan wordt met het verwerken van (persoons)gegevens. In 2019 wordt daarmee verder gegaan. Het streven is om in het voorjaar van 2019 alle PIA's uitgevoerd te hebben, zodat de rapportages daarover met bevindingen, conclusies en aanbevelingen vastgesteld kunnen zijn op 25 mei 2019....als de AVG één jaar geldt.

Het register en de PIA's zijn nog niet volledig afgerond, waarmee niet alle verplichtingen uit de AVG volledig geïmplementeerd zijn. Dit betekent niet dat de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens) direct handhavend zal optreden en een forse boete gaat opleggen. Als aangetoond kan worden dat de Gemeente Barneveld zich bewust is van deze verplichtingen en niet achterover leunt, maar een concrete datum kan noemen waarop ook aan deze verplichtingen van de AVG is voldaan, is de kans nihil dat de Autoriteit Persoonsgegevens de Gemeente Barneveld daarop zal aanspreken.

Overigens moet 25 mei 2018 niet gezien worden als een einddatum, waarop alles op het gebied van privacy echt 'klaar' is. Dit is immers een vakgebied dat continue in beweging is en steeds onder de aandacht zal blijven. Verwerkersovereenkomsten, het register en de verschillende overzichten zijn altijd aan veranderingen onderhevig. Er dient continue aandacht besteed te worden aan privacy van burgers, bedrijven en medewerkers, waarbij een zorgvuldige verwerking van de persoonsgegevens en de bescherming daarvan steeds gewaarborgd moeten zijn. Daarbij is het belangrijk het bewustzijn van dit belang goed onder de aandacht te hebben en te houden.

Kortom, de Gemeente Barneveld heeft in 2018 hard gewerkt om aan de vereisten die de AVG stelt te voldoen en er is veel gerealiseerd.

2. WETTELIJK KADER

2.1 AVG Algemeen

Op 25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening voor de verwerking van persoonsgegevens kent een rechtstreekse werking voor de lidstaten en is in de plaats gekomen van de Wet bescherming persoonsgegevens. In de AVG worden de rechten van burgers versterkt en de AVG legt de nadruk op de eigen verantwoordingsplicht van organisaties die persoonsgegevens verwerken. Dit betekent dat organisaties bijvoorbeeld goed moeten vastleggen welke gegevens zij verwerken, met welk doel, hoe lang zij die gegevens bewaren, dat zij de gegevens goed beveiligen en met wie ze gegevens delen. De rechtstreekse werking van de AVG zorgt ervoor dat de regels voor bescherming van persoonsgegevens uniform zijn binnen de Europese Unie.

De AVG geeft een overkoepelend kader voor het verwerken van persoonsgegevens en is nader uitgewerkt in de Nederlandse Uitvoeringswet AVG. Daarnaast zijn er in materiewetgeving, zoals de Jeugdwet, de Wet maatschappelijke ondersteuning en de Wet basisregistratie personen, specifieke regels te vinden voor het verwerken van persoonsgegevens. De AVG hangt daar altijd als een paraplu boven. Dat betekent dat als persoonsgegevens verwerkt mogen worden op grond van de materiewetgeving, de bepalingen van de AVG daar boven blijven hangen. Er moet bijvoorbeeld altijd een rechtmatige grondslag zijn voor het verwerken van persoonsgegevens en persoonsgegevens mogen alleen worden verwerkt voor het doel waarvoor ze zijn verzameld.

2.2 Specifieke wetgevende ontwikkelingen en jurisprudentie

Door de Autoriteit Persoonsgegevens (AP) wordt regelmatig onderzoek gedaan naar de verwerking van persoonsgegevens en de naleving van privacywetgeving in specifieke situaties. Deze onderzoeken worden veelal gepubliceerd en geven meer inzicht in de wijze waarop de AP regelmatig richtsnoeren of uitspraken die relevant kunnen zijn voor een juiste toepassing van privacyregels. In 2018 heeft de AP verschillende onderzoeken gedaan, belangrijke onderzoeken zijn bijvoorbeeld:

- Onderzoek naar de verwerking van BSN in BTW-nummers door de Belastingdienst, juni 2018;
- Onderzoeken gegevensverwerking gemeente Nijmegen en gemeente Zaanstad (over het gebruik van de zelfredzaamheidsmatrix in het sociaal domein), februari 2018.

Daarnaast worden door de European Data Protection Board, voorheen Working Party 29, de samenwerking van alle nationale privacytoezichthouders van de Europese Unie (EDPB), regelmatig guidelines gepubliceerd die meer richting kunnen geven aan de juiste toepassing van de AVG. Belangrijke guidelines die de EDPB over de AVG heeft gepubliceerd zijn bijvoorbeeld:

- Guidelines on Data Protection Impact Assessments (wp248rev.01): van belang bij of wanneer een Data Protection Impact Assessment moet worden uitgevoerd;
- Guidelines on Data Protection Officers (DPO'S)(wp243rev.01): over de rol van de Functionaris Gegevensbescherming;
- Guidelines on consent under Regulation 2016/679 (wp259rev.01): over het gebruik van toestemming als rechtmatige grondslag.

2.3 Toezichtskader AP: ontwikkelingen en gevolgen

De Autoriteit Persoonsgegevens (AP) heeft in mei 2018 haar toezichtkader voor 2018 en 2019 gepubliceerd. In dit kader geeft de AP haar prioriteiten aan voor de komende periode.

Bevordering naleving van de privacywetgeving

Het belangrijkste doel van het toezicht van de AP is de bevordering van de naleving van de privacywetgeving. Dit doel wil de AP onder meer bereiken door het bieden van 'guidance'. De AP geeft als voorbeelden het geven van voorlichting en advies aan mensen en organisaties, het aanbieden van praktische hulpmiddelen, het aanbieden van een duidelijke normuitleg en het bevorderen van de totstandkoming van Europees gedragen normen.

De AP legt daarnaast de nadruk op de behandeling van klachten, omdat het klachtrecht onder de AVG is versterkt en het behandelen van klachten de naleving van de privacywetgeving kan bevorderen. Hiervoor heeft de AP een Informatie- en Meldpunt Privacy ingesteld. De AP neemt klachten in behandeling die wijzen op een mogelijke inbreuk op de verwerking van persoonsgegevens van mensen en wil betrokkenen hiermee versterken in hun rechten.

Controle op de naleving van de AVG

De verantwoordingsplichten in de AVG dwingen organisaties aan te tonen dat zij voldoen aan de AVG. Om vast te stellen dat aan de verantwoordingsplichten van de AVG is voldaan, wordt in de verschillende sectoren de naleving van één van deze verplichtingen gecontroleerd. Daarbij kan bijvoorbeeld gedacht worden aan de controle of een verplichte Functionaris gegevensbescherming is aangesteld, of er een register van verwerkingen is en een register wordt bijgehouden van beveiligingsincidenten en de genomen maatregelen. Het op orde hebben van de verantwoordingsplichten is volgens de AP een goede indicatie van de mate waarin serieus werk is gemaakt van de implementatie van de AVG en dat is nagedacht over belangrijke onderdelen uit de AVG (zoals grondslagen, doelbinding en beveiliging).

Risicogericht toezicht

De AP geeft in haar toezichtkader aan dat zij een risicogerichte aanpak gaat hanteren en daarbij extra oog heeft voor mogelijke inbreuken op de bescherming van persoonsgegevens waarbij grote groepen mensen kunnen worden geraakt. Daarbij

richt zij zich de komende periode in het bijzonder op de overheid, de zorg en bedrijven die handelen in persoonsgegevens. Voor de overheid geldt dat de AP extra focus gaat leggen op zowel de beveiliging van persoonsgegevens als de vraag of de verwerking van de persoonsgegevens is gebaseerd op de juiste grondslag. De AP gaat daarvoor bijvoorbeeld controles uitvoeren op de naleving van de verplichtingen om een register van verwerkingen op te stellen, de verplichting een Functionaris gegevensbescherming (FG) aan te stellen (deze controle is voor gemeenten reeds uitgevoerd in 2018), alsmede de wijze waarop de organisatie de FG positioneert en hem in staat stelt de taken en verplichtingen uit te voeren die hij op grond van de AVG heeft.

Datalekken
De AVG stelt een aantal nieuwe eisen aan de meldplicht datalekken. Organisaties moeten bijvoorbeeld alle datalekken documenteren en niet alleen de gemelde datalekken. Zij moeten een register van datalekken bijhouden. De AP geeft het komende jaar extra aandacht aan niet-gemelde datalekken en datalekken die (mede) zijn veroorzaakt door ernstige tekortkomingen in de beveiliging.

3. GOVERNANCE

3.1 Governance algemeen

Er is een duidelijke structuur aangaande de governance aanwezig wat betreft de uitvoering van de AVG. Er zijn een (interim) Chief Information Security Officer (CISO), een Privacy Officer (PO) en een Functionaris Gegevensbescherming (FG) aangewezen door het college. Deze onderlinge relaties en verantwoordingen blijken uit het door het college vastgestelde Privacybeleid dat op 1 april 2018 in werking is getreden. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient aan te kunnen tonen 'in control' te zijn aangaande de uitvoering van de AVG.

3.2 Verantwoording Functionaris gegevensbescherming

Overzicht uitgevoerde werkzaamheden in 2018:
In maart 2018 heeft het college het Privacybeleid vastgesteld. Dit beleid is te vinden op de gemeentelijke website. Er zijn in april en mei 2018 diverse bijeenkomsten georganiseerd over de AVG voor de welzijnsorganisaties en vrijwilligersorganisaties om ook deze organisaties bewust te maken van het belang van de AVG.

In de periode vanaf oktober 2018 zijn de eerste Privacy Impact Assessments (PIA's) uitgevoerd. Daarbij wordt ernaar gestreefd om deze in het eerste kwartaal van 2019 af te ronden, zodat rond eind mei – als de AVG een jaar van toepassing is – de PIA rapportage afgerond en vastgesteld is. Het tweede halfjaar van 2019 kan vervolgens gebruikt worden om de uit de PIA's voortvloeiende acties op te pakken en uit te voeren. Van een tweetal te verlengen danwel uit te voeren pilots binnen het Sociaal Domein zijn de PIA's als eerste uitgevoerd en zijn c.q. worden de rapportages in december 2018 resp. februari 2019 vastgesteld. Deze PIA's zijn in samenwerking met de convenantpartners uitgevoerd, zodat alle partijen direct bekend zijn met de risicofactoren en hoe voorafgaande aan de (verlenging van) de pilot daarop ingespeeld kan worden, zodat de bescherming van de verwerking en deling van (persoons)gegevens voldoende gewaarborgd is.

3.3 Verantwoording Privacy Officer

Overzicht uitgevoerde werkzaamheden in 2018:

Openbaarmaking persoonsgegevens middels besluitenlijsten, raadstukken etc.	Voor het publiceren van persoonsgegevens op de website zijn afspraken gemaakt en is een memo geschreven met een voorstel voor richtlijnen.
PIA's uitvoeren	In het najaar van 2018 is de PIA uitgevoerd op 8 processen, met name in het sociaal domein, belastingen en veiligheid.
Overige vereisten uit de AVG invoeren	Privacy by design en default is vanaf mei 2018 bij nieuwe applicaties als eis meegenomen.

Bewustwording privacy en informatiebeveiliging	- Samen met de CISO zijn workshops voor medewerkers verzorgd. - Op verzoek zijn de CISO of PO bij teamoverleggen aanwezig geweest. - Met campagnemateriaal is bewustwording gecreëerd. - Periodiek is een nieuwsbericht op intranet gezet.
Privacy en Publiekszaken	In overleg met Publiekszaken is ondersteuning geboden bij privacyvraagstukken en het updaten van de Verordening gegevensverstrekking BRP en onderliggende reglementen.
Verwerkersovereenkomsten	Alle contracten zijn gecontroleerd en waar nodig zijn verwerkersovereenkomsten opgesteld of aangepast. Daarnaast is er een factsheet over verwerkersovereenkomsten op intranet gezet. Met nieuwe verwerkers zijn verwerkersovereenkomsten gesloten.
Informeren gemeenteraad	De raad is bij memo geïnformeerd en de Commissie Bestuur is op 19 juni 2018 bijgepraat door de portefeuillehouder. Op 30 oktober 2018 heeft de raadscommissie Bestuur een update ontvangen over de afronding van het register van verwerkingen, de verwerkersovereenkomsten en de plannen voor het najaar van 2018.
Instellen + vullen register van verwerkingen	Het register van verwerkingen is bijna afgerond. Nieuwe processen en wijzigingen worden hieraan toegevoegd.
Ondersteunen bij ontwikkelingen dienstverlening	Bij het ontwikkelen van nieuwe / andere vormen van de dienstverlening van Barneveld is de privacyregelgeving meegenomen.
Privacy en Sociaal domein	Waar mogelijk is begeleiding geboden in de noodzakelijke omwentelingen binnen het Sociaal Domein op het gebied van de privacyregelgeving.
Inrichten intranet	Algemene informatie over privacy, informatiebeveiliging en werkinstructies is op intranet geplaatst.
Proces omtrent datalekken inregelen en monitoren	Dit proces is opgesteld en wordt gemonitord. Inbreuken in verband met privacy zijn geregistreerd. Datalekken zijn gemeld bij de AP.
Instellen FG	De FG van de gemeente Scherpenzeel is per 1 mei 2018 ook aangesteld als FG van de gemeente Barneveld.
Instellen PO	Op 1 augustus 2018 is de nieuwe PO gestart. Deze PO heeft uitvoering gegeven aan: - Toetsen / opstellen verwerkersovereenkomsten - Behandelen privacy vraagstukken - Signaleringsfunctie in organisatie
Opstellen privacy statement website	Het privacy statement is bijgewerkt om burgers te informeren op welke wijze door de gemeente Barneveld wordt omgegaan met privacy en welke rechten zij als burgers hebben.

3.4 Verantwoording CISO

Overzicht uitgevoerde werkzaamheden in 2018:

Bewustwording privacy en informatiebeveiliging	- Samen met de PO zijn workshops voor medewerkers verzorgd. - Op verzoek zijn de CISO of PO bij teamoverleggen aanwezig geweest. - Met campagnemateriaal is bewustwording gecreëerd. - Periodiek is een nieuwsbericht op intranet gezet.
Inrichten intranet	Algemene informatie over privacy, informatiebeveiliging en werkinstructies is op intranet geplaatst.
Zelfevaluatie BRP/PNIK	Ieder jaar draagt de Gemeente Barneveld een verantwoording af over BRP / PNIK wetgevingen.
Zelfevaluatie ENSIA	Ieder jaar draagt de Gemeente Barneveld een verantwoording af over informatiebeveiliging door middel van ENSIA (Eenduidig Normatiek Single Information Audit). Hierin vallen ondermeer BAG, BGT, DigiD, Suwinet en BIG. Sinds 2018 valt daaronder ook de verantwoording over AVG. Daarbij worden DigiD, Suwinet en ENSIA overall getoetst door een RE/RA auditor.
BIG-BIO transitie	Vanaf 2020 geldt voor alle overheidsinstanties de BIO, hiervoor is een transitieslag gaande.

4. WERKZAAMHEDEN EN BEVINDINGEN

4.1 Privacybeleid

Begin 2018 is het Privacybeleid herzien en in maart 2018 is door het college het nieuwe beleid vastgesteld. Op 1 april 2018 is het nieuwe Privacybeleid in werking getreden. Op 30 mei 2018 is de gemeenteraad hierover geïnformeerd. Dit beleid implementeert de uitgangspunten en verplichtingen uit de AVG. De uitgangspunten rechtmatigheid, behoorlijkheid, transparantie, doelbinding, subsidiariteit, proportionaliteit, dataminimalisatie en vertrouwelijkheid worden omgezet in alle werkprocessen waarbinnen persoonsgegevens worden verwerkt. Er is beleid gevormd op hoe om te gaan met de rechten van betrokkenen, meldplicht datalekken, de functies van FG, PO en CISO en de gegegevensuitwisseling tussen verschillende domeinen en afdelingen. Eind 2018 is een begin gemaakt met het formuleren van aandachtspunten vanuit privacy in het gemeentebrede cloudbeleid.

4.2 Register van verwerkingen

Alle werkprocessen zijn gedurende 2018 geanalyseerd op de verwerking van persoonsgegevens en in overleg met bijna alle teams is het register van verwerkingen opgesteld. Er ontbreken nog enkele processen in het register. Deze worden begin 2019 aangevuld.

4.3 Meldingen datalekken

In totaal zijn er in 2018 34 beveiligingsincidenten gemeld. Nader onderzoek wijst uit dat er 11 beveiligingsincidenten gemeld moesten worden aan de AP. Hierbij zijn in alle 11 de gevallen betrokkenen geïnformeerd. Uit een analyse van de datalekken is bepaald dat er meer bewustwording moet worden gegeven over omgang met bedrijfsmiddelen. Daarnaast zijn er technische maatregelen getroffen om de gebruikers te ondersteunen.

4.4 Rechten van betrokkenen

In 2018 is het proces rond de rechten van betrokkenen verbeterd. In de privacyverklaring op de website is informatie opgenomen voor betrokkenen. De mogelijkheden tot het indienen van een verzoek of klacht zijn op de website voorzien. Er zijn formats opgesteld voor de ontvangstbevestiging, afwijzing en toewijzing van een verzoek. Ook is een stroomschema opgesteld hoe een verzoek behandeld moet worden. Er zijn in 2018 geen verzoeken binnengekomen. Er is in 2018 1 klacht in verband met privacy ingediend. Deze klacht is naar tevredenheid afgehandeld.

4.5 Bewaartermijnen

Op 11 oktober 2018 heeft team DIV de "Bezemdag" georganiseerd. Tijdens deze dag zijn veel papieren dossiers gearchiveerd of vernietigd. Ook is tijdens deze dag aandacht gevraagd voor het bewaren van persoonsgegevens in Outlook en op de harde schijf. Digitale dossiers en bijbehorende documenten en metadata worden door team DIV verwijderd na het verstrijken van de wettelijke bewaartermijnen. In overleg met team DIV is een start gemaakt met het project "Digitaal bezemen" om te zorgen dat op de harde schijven van medewerkers geen persoonsgegevens langer dan

toegestaan bewaard blijven. Dit aandachtspunt wordt nadrukkelijk meegenomen in de Privacy Impact Assessments (PIA's). Er is overleg gevoerd over het opschonen van persoonsgegevens in de diverse applicaties. Bij nieuwe applicaties wordt de eis van automatisch verwijderen meegenomen.

4.6 Verwerkers en verwerkersovereenkomsten

In 2018 is met een groot aantal bestaande verwerkers een (nieuwe) verwerkers-overeenkomst afgesloten. Ook zijn er tientallen nieuwe verwerkersovereenkomsten bijgekomen. Een actueel overzicht hiervan is beschikbaar. Bestaande verwerkers hebben niet gerapporteerd over incidenten. De controle op de naleving van de verwerkersovereenkomst zal medio 2019 plaatsvinden.

4.7 Privacy in het Sociaal Domein

De Privacy Officer heeft in 2018 de afdeling Sociaal Domein veel geadviseerd over de verwerking van persoonsgegevens, bij de aanschaf van nieuwe applicaties, bij gegevens-uitwisseling tussen deze afdeling en andere afdelingen en tussen de verschillende wetten. Er is een memo opgesteld over integrale aanpak in relatie tot beschermd werken, waarin de risico's in kaart zijn gebracht van gegevensuitwisseling vanuit de Participatiewet naar de WMO en vice versa en de rolvermenging die daarbij optreedt. De maatregelen om risico's te mitigeren zijn: logging en steekproefsgewijze monitoring van Suite voor WMO, workshop voor de medewerkers met twee rollen over de eisen die de AVG en de WMO stelt aan inzage en verwerking van gegevens en het uitdrukkelijk vragen van toestemming van de klant.

De samenwerking met andere gemeenten in het Sociaal Domein in de regio FoodValley is in 2018 bestendigd. Speciale aandacht is er voor gegevensuitwisseling met andere gemeenten. Voor het WerkgeversServicePunt is een begin gemaakt met het opstellen van een convenant met een privacyparagraaf. Voor de samenwerking Jeugdhulpregio FoodValley is een Privacyregelement opgesteld, dat echter nog niet voldoende waarborgen bidet, zodat hierover in 2019 wordt dooronderhandeld. Voor het Platform regionale samenwerking huisvesting statushouders is een privacyreglement in de maak. Met diverse verwerkers zijn verwerkersovereenkomsten gesloten. Met de gemeente Ede is een verwerkersovereenkomst gesloten voor de machtiging van een medewerker voor de gemeente Barneveld tot de Collectieve Opdracht Routeer Voorziening (CORV).

Voor de samenwerking met Vluchtelingenwerk Nederland en Welzijn Barneveld is een convenant of privacyregelement opgesteld. Voor de samenwerking met Woningstichting Barneveld wordt gewerkt aan een convenant dat naar verwachting in februari 2019 ondertekend wordt.

In 2018 is de website van Welzijn Barneveld gehackt en heeft er een datalek plaatsgevonden. Hierbij is vastgesteld dat er geen persoonsgegevens zijn ingezien die ter uitvoering van het mantelzorgcompliment zijn verwerkt. Van deze datalek heeft Welzijn Barneveld melding gedaan bij de AP.

Er is in 2018 een privacyprotocol opgesteld voor de samenwerking onder het convenant *"Het tegengaan van identiteitsfraude en documentenfraude Oost-Nederland".*

De samenwerking met team Veiligheid vindt plaats in het Veiligheidshuis West Veluwe Vallei en sinds december 2018 in het MDO verward gedrag. Op 5 december 2018 is door de gemeente en een groot aantal partners in het zorg- en veiligheidsdomein het convenant *"Sluitende Aanpak Personen met Verward Gedrag"* en bijbehorend privacyreglement ondertekend.

4.8 Informatieveiligheid

De CISO is druk bezig geweest met het opleveren van de verantwoordingen in het kader van BAG, BGT, DigiD, Suwinet, BIG, ENSIA, BRP en PNIK. Daarnaast zijn er tal van maatregelen geëvalueerd (en eventueel bijgestuurd). De CISO acteert op alle lagen van de Gemeente Barneveld (Strategisch, Tactisch en Operationeel). De CISO stelt zowel beleidsstukken op als dat de CISO langs verschillende teams gaat voor bewustwordingstrainingen. Op dit moment voldoet de Gemeente Barneveld aan alle wettelijke verplichtingen rondom informatiebeveiliging.

4.9 Data Privacy Impact Assessments

In 2018 zijn er acht Privacy Impact Assessments gehouden:

- Voor het team Veiligheid voor de volgende werkprocessen: de BOA's (o.a. BRS), ondermijning (RIEC), evenementen en Damocles.
- Rioolaansluitingen
- Heffingen- en invorderingsadministratie
- Urgentieverklaring wonen

Voor de pilot Vroegsignalering schuldhulp is een voorafgaande PIA gehouden.

Voor de volgende onderwerpen is afgesproken in het voorjaar van 2019 een PIA te houden:

- Veiligheid: Wet BIJ, Horeca
- Sociaal domein: Jeugdhulp, Onderwijs – Leerlingenvervoer / Leerplicht, WMO - materiële hulp / immateriële hulp, Participatiewet / IOAW / IOAZ
- Applicaties: Suite4Sociaal Domein, Key2begraven, SUWI-net, Stroomlijn, Stratech, Key2Jongerenmonitor, Atlantis, Verseon, Outlook

De PIA's vonden plaats aan de hand van de vragenlijst van de beroepsvereniging voor IT-auditors NOREA. Hierin wordt gevraagd naar de verwerkingsverantwoordelijke en verwerkers(overeenkomsten), nieuwe technieken, noodzaak van gegevensverwerking, aard van de persoonsgegevens (bijzonder of gevoelig), gegevensuitwisseling intern en extern, doelbinding, grondslag, transparantie, actualiteit, integriteit en beschikbaarheid van persoonsgegevens, rechten van betrokkenen, bewaartermijnen en beveiliging.

Per team wordt een rapportage opgesteld met bevindingen, conclusies en aanbevelingen. Wanneer een werkproces op korte termijn gewijzigd wordt of als sprake is van een pilot, wordt een aparte rapportage opgesteld.

In de gehouden PIA's komen de volgende risico's naar voren:

1. De aanwezigheid van een schaduwarchief. Als de gegevens (gegevens en alle documenten) te lang worden bewaard, houdt dit in dat er een risico is op onrechtmatig gebruik (voor andere doelen) of verlies van gegevens.
2. Er worden gegevens onbeveiligd verzonden per e-mail.
3. Er worden gevoelige gegevens bewaard in een algemeen toegankelijke map op de P-schijf.
4. Deelname van de Woningstichting aan een adviescommissie, waardoor het risico aanwezig is dat de gegevens voor andere doeleneinden gebruikt worden. Daarnaast bewaart WSB de gegevens en documenten permanent en is niet bekend op welke wijze de beveiliging van de documenten en systemen is geregeld.

De volgende maatregelen zijn reeds genomen:

1. Het team DIV heeft op de gemeentewerf een actie gehouden om het (schaduw)archief te verwerken en op te schonen.
2. Er wordt beveiligd gemaild met een wachtwoord.
3. Er wordt gewerkt aan een convenant met de WSB om afspraken te maken over doelbinding en bewaartermijnen.

Er zijn afspraken gemaakt over de termijn waarop andere maatregelen worden genomen.

4.10 Bewustwording

Meer bewustwording van privacyrisico's onder medewerkers is in 2018 op verschillende manieren gestalte gegeven. In maart, juni, september en december zijn workshops over Privacy en Informatiebeveiliging gehouden. Deze workshop is verplicht voor alle nieuwe medewerkers. De medewerkers van de afdeling Sociaal Domein hebben daarnaast de algemene workshop en een workshop over beveiligd mailen gevolgd. In januari en februari 2019 worden er specifiek op het sociaal domein gerichte trainingen Privacy en Informatieveiligheid gegeven. Er is campagnemateriaal ontwikkeld met regels over privacy. De Privacy Officer is regelmatig aanwezig geweest bij teamoverleggen, bij overleggen van de personeelsvereniging en de OR om vragen op gebied van privacy te beantwoorden. Ook is periodiek een bericht op intranet gezet met tips om privacy op het netvlies te houden. Belangrijk voor de bewustwording is ook de bekendheid en benaderbaarheid van de PO om als vraagbaak te fungeren. Hiervan is veel gebruik gemaakt.

5. AANBEVELINGEN EN ACTIES

5.1. Aanbevelingen

Belang: het is belangrijk om het bewustzijn over het belang van het zorgvuldig omgaan met en verwerken van persoonsgegevens blijvend onder de aandacht te houden bij de medewerkers. Daarbij is de combinatie privacy en informatieveiligheid een vast gegeven.

Aanbeveling: voor een blijvend bewustzijn regelmatig berichten op intranet plaatsen. Ook kan met de teamleiders afgesproken worden dat de Privacy Officer met enige regelmaat of incidenteel aanschuift bij teamoverleggen om in algemene zin of aan de hand van een specifieke casus het bewustzijn over het omgaan met persoonsgegevens hoog te houden.

Belang: bij aanschaf van nieuwe of te vernieuwen software, applicaties en diensten een PIA uit te voeren om vooraf een risico-inschatting te kunnen maken. Dit geldt ook voor hardware en apparatuur zoals printers en papiervernietigers indien het betreffende apparaat beschikt over een eigen harde schijf waarop gegevens opgeslagen kunnen worden. Ook moet behalve een overeenkomst van opdracht/levering een verwerkersovereenkomst afgesloten worden.

Aanbeveling: nog beter onder de aandacht brengen bij de mederwerkers dat deze twee overeenkomsten onlosmakelijk met elkaar verbonden zijn en dat deze overeenkomsten voorafgaande aan de levering of uitvoering van de dienst afgesloten moeten zijn. In samenwerking met de CISO kan hier goed zicht op gehouden worden.

Belang: zorgvuldige verwerking en deling van (persoons)gegevens met convenantpartners in geval een pilot opgestart wordt.

Aanbeveling: indien het wenselijk is om een pilot (veelal met andere partijen) uit te gaan voeren, is het van belang vooraf een PIA uit te voeren en een convenant of samenwerkingsovereenkomst af te sluiten. Dit om goede afspraken te maken voordat een pilot van start gaat en om daarmee problemen tijdens of na de pilot zoveel mogelijk te voorkomen en om vooraf duidelijk te hebben wie welke taken en verantwoordelijkheden heeft voor het geval er problemen ontstaan.

5.2. Acties voor 2019

In de voorgaande hoofdstukken is aangegeven welke werkzaamheden in 2018 zijn uitgevoerd en in paragraaf 5.1. worden de aanbevelingen genoemd. In deze laatste paragraaf wordt nader ingegaan op de acties die hiervoor al kort genoemd zijn. In 2019 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2019 gerapporteerd zal worden.

- Afronding van het register van verwerkingen, omdat deze nog niet geheel volledig is (circa 90%).
- Vervolg uitvoering PIA's. Streefdatum vastgestelde rapportage: 25 mei 2019.
- Continue aandacht houden voor het belang van het afsluiten van verwerkersovereenkomsten en het overzicht actueel houden. Verouderde overeenkomsten actualiseren en nieuwe overeenkomsten afsluiten met nieuwe verwerkers.
- Vervolg workshops Privacy & Informatieveiligheid voor nieuwe medewerkers.
- Aanvullende specifieke workshops voor vakgebieden, waarin veel (persoons)gegevens verwerkt worden. In overleg met de teamleiders bespreken welke vakgebieden daarvoor in aanmerking komen.
- Vervolg opschoonacties, waarbij de wettelijke bewaartermijnen goed in acht genomen moeten worden. Bij het opschonen van documenten en (persoons)gegevens, inclusief metadata, moet niet vergeten worden dat veel medewerkers schaduwbestanden hebben in ordners en op netwerkschijven. Ook de gegevens en documenten in e-mailberichten mogen daarbij niet vergeten worden.
- Dooronderhandelen over privacyreglement Jeugdhulpregio Foodvalley, zodat voldoende waarborgen in het privacyreglement worden opgenomen.
- Diverse convenanten, die nog in onderhandeling zijn, afsluiten en ondertekenen, nadat er voldoende waarborgen in opgenomen zijn waarmee voldaan wordt aan de AVG vanuit privacy oogpunt. En waarmee eveneens aan de minimale normen voldaan wordt voor Informatieveiligheid zoals ISO 27001/27002 c.q. BIG-BIO en een procedure voor het analyseren en beoordelen van beveiligingsincidenten en het melden van datalekken.

gemeente
Barneveld

Memo

Datum:
7 februari 2019

Onderwerp: Jaarverslag Functionaris Gegevensbescherming 2018

Ter attentie van: Gemeenteraad

Afzender: College van Burgemeester en wethouders

Geachte leden van de gemeenteraad,

Op grond van de Europese Algemene Verordening Gegevensbescherming (AVG), die per 25 mei 2018 de Wet bescherming persoonsgegevens heeft vervangen, en het Privacybeleid brengt de Functionaris Gegevensbescherming (FG) jaarlijks voor 1 maart verslag uit aan de bestuursorganen. In het verslag is toegelicht hoe de Gemeente Barneveld de AVG heeft geïmplementeerd en omgaat met de persoonsgegevens van inwoners, bedrijven en instanties. Dit verslag bevat informatie over de verantwoording van de verschillende functionarissen, de werkzaamheden en bevindingen, aanbevelingen en de te ondernemen acties voor het volgende jaar.

Implementatie AVG en omgang met persoonsgegevens
Het verslagjaar ziet op de periode van 1 januari tot en met 31 december 2018. In de verslagperiode is hard gewerkt om aan de verplichtingen van de AVG te voldoen. Zo zijn de volgende zaken (nagenoeg) gerealiseerd:

- aanstelling Functionaris Gegevensbescherming;
- aanstelling Privacy Officer;
- een register van verwerkingen (90% gereed);
- een privacyverklaring (voor op de website);
- een overzicht van de verwerkersovereenkomsten, het afsluiten van vele nieuwe of geactualiseerde verwerkersovereenkomsten;
- een overzicht van de rechten van betrokkenen (voor op de website);
- het uitvoeren van Privacy Impact Assessments (50% gereed);
- een overzicht van de voorgekomen beveiligingsincidenten en datalekken;
- een Privacybeleid en;
- bewustwording van medewerkers (door verplicht gestelde workshops en berichten op intranet).

Het register en de PIA's zijn nog niet volledig afgerond, waarmee niet alle verplichtingen uit de AVG volledig geïmplementeerd zijn. Dit betekent niet dat de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens) direct handhavend zal optreden en een forse boete gaat opleggen. Als aangetoond

kan worden dat de Gemeente Barneveld zich bewust is van deze verplichtingen en niet achterover leunt, maar een concrete datum kan noemen waarop ook aan deze verplichtingen van de AVG is voldaan, is de kans nihil dat de Autoriteit Persoonsgegevens de Gemeente Barneveld daarop zal aanspreken.

Overigens moet 25 mei 2018 niet gezien worden als een einddatum, waarop alles op het gebied van privacy echt klaar is. Dit is immers een vakgebied dat continue in beweging is en steeds onder de aandacht zal blijven. Verwerkersovereenkomsten, het register en de verschillende overzichten zijn altijd aan veranderingen onderhevig. Kortom, er dient continue aandacht besteed te worden aan privacy van burgers, bedrijven en medewerkers, waarbij een zorgvuldige verwerking van de persoonsgegevens en de bescherming daarvan steeds gewaarborgd moeten zijn. Daarbij is het belangrijk het bewustzijn van dit belang goed onder de aandacht te hebben en te houden.

U treft ter kennisname het jaarverslag aan.