Gemeente Woudenberg

Collegeadvies Eigen initiatief

Besluitenregistratie:		Postregistratienummer : 206485
18	10	Datum inboeken :

Openbaar	Ja	**Internet**	Nee
naar RAAD	Nee	**OR**	Nee
Communicatie	Nee	**Europese regelgeving**	Nee
via COMMISSIE	~~Nee~~ Ja		
Anders:			

Onderwerp : Vaststelling gemeentelijk privacybeleid in het kader van de Algemene Verordening Gegevensbescherming. (AVG)

Advies :
1. Vaststellen bijgevoegde privacyverklaring website;
2. Vaststellen bijgevoegd privacyreglement/privacybeleid;
3. Collegeadvies ter informatie naar raadscommissie zenden.

Datum	Ambtenaar	Afdeling	Pho	Griffier	Afdelings-hoofd
30-04-2018	L. Vos	K&A			

Additioneel Advies	Paraaf:
N.V.T.	

	Conform advies	Bespreken	Datum	Opmerkingen
Burgemeester			30/4	
Wethouder			02/05	
Wethouder			8/5	
Secretaris			1/5	

Datum vergadering B&W: **Agendapunt:**

Besluit:

08 MEI 2018

Retour naar afdeling op:

Ter archivering aangeboden op:

Inleiding
Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie.

Centrale vraag
Kan het college instemmen met het vaststellen van de privacyverklaring voor de website en het privacyreglement/privacybeleid?

Beoogd resultaat (wat)
Voldoen aan de wettelijke eisen van de AVG.

Kader
-AVG

Argumenten
De implementatie van de AVG is al een tijd in volle gang. In 2017 heeft de prioriteit gelegen bij het tijdig (1 januari 2018) op orde krijgen van de nieuwe Coöperatie De Kleine Schans inclusief alle maatregelen waarom de AVG vraagt. Dit houdt in dat voor de eigen organisatie vóór 25 mei 2018 nog een aantal stappen gezet moesten worden. Dit betreft onder andere het vaststellen van de privacyverklaring voor de website en het vaststellen van het gemeentelijk privacybeleid- met onderliggend reglement. Deze stukken zijn voorbereid en opgesteld door de gemeentelijke CISO en FG. Voor de privacyverklaring website is gekeken naar de manier waarop de gemeente Amersfoort deze heeft vormgegeven. Voor het privacybeleid is als uitgangspunt het VNG-model genomen. Deze voldoet aan alle vereisten die de AVG stelt.

Beide stukken worden u aangeboden in uw bevoegdheid als college. Daarnaast vraagt de AVG ook om een aantal andere zaken die geregeld moeten worden. Het lijkt mij goed om u in dit kader te informeren over de maatregelen die getroffen zijn om voorbereid te zijn op de nieuwe privacywetgeving. Bij de implementatie van de AVG is aangesloten bij het 10-stappenplan dat de Autoriteit Persoonsgegevens als leidraad mee geeft.

1. *Bewustwording:*

De implementatie van de AVG vraagt om een extra stuk bewustwording van iedereen die met privacygevoelige (persoonsgegevens) omgaat. Medewerkers moeten inschatten wat de impact van de AVG is op de huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Hierin ligt een belangrijke taak voor de gemeentelijke Functionaris Gegevensbescherming.

Actie: Voor medewerkers is een 'Beslisboom wel of geen verwerkersovereenkomst' opgesteld. Hierin is op schematische wijze weergegeven waaraan gedacht moet worden als er privacygevoelige gegevens worden verwerkt. Bewustwording blijft een structureel aandachtspunt en is nooit af.

2. *Rechten van betrokkenen:*

Onder de AVG krijgen mensen van wie persoonsgegevens worden verwerkt meer en verbeterde privacyrechten. Dit betreft onder meer al bestaande rechten zoals het recht op inzage, correctie en verwijdering. Maar ook het recht op dataportabiliteit. Dit houdt in dat betrokkenen hun gegevens makkelijk kunnen opvragen en vervolgens kunnen meenemen naar een andere organisatie.

Actie: Op de ICT-markt zijn momenteel meerdere tools in ontwikkeling om als organisatie ook daadwerkelijk een beroep op b.v. het recht van dataportabiliteit aan te kunnen. Persoonsgegevens zijn immers vaak in meerdere systemen opgeslagen. Wij zijn momenteel in gesprek met een aanbieder van een beheertool om te kunnen voldoen aan de nieuwe eisen.

3. *Overzicht verwerkingen:*

Op 25 mei 2018 moet er een overzicht van alle gegevensbewerkingen in onze organisatie zijn. Wij moeten kunnen aantonen welke gegevens wij verwerken, voor welk doel wij deze nodig hebben (doelbinding), welke wettelijke grondslag wij hebben (rechtmatigheid) en wie binnen de gemeente toegang heeft tot deze gegevens. Om onze verwerkingen in kaart te brengen hebben wij onderzoek door BMC-adviseurs uit laten voeren. Dit register is noodzakelijk in het kader van de verantwoordingplicht richting de Autoriteit Persoonsgegevens.

Actie: Het verwerkingenregister is op 25 mei 2018 actueel. Om dit zo te houden is een beheertool nodig. We zijn op dit moment in gesprek met een leverancier om te kunnen voldoen aan de nieuwe eisen.

4. *Data protection impact assessment (DPIA)*

Onder de AVG kan het verplicht zijn een DPIA uit te voeren. Dit houdt in dat applicaties waarin gegevens worden verwerkt met een hoog privacyrisico getoetst worden aan de AVG om vooraf de privacyrisico's van gegevensverwerkingen in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

Actie: Op 25 mei 2018 hoeven nog niet alle applicaties onderworpen te zijn geweest aan een DPIA. Ook hiervoor geldt dat het nog zoeken is naar een beheerstool waarmee deze controltaak op een efficiënte manier uitgevoerd kan worden. Wij zijn hierover in gesprek met een leverancier. In de loop van het jaar zullen allereerst de kernapplicaties waarin gegevensverwerkingen plaatsvinden onderworpen worden aan een DPIA.

5. *Privacy by design en privacy by default*

Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten er voor gezorgd wordt dat persoonsgegevens goed worden beschermd. Privacy by default houdt in dat er technische en organisatorische maatregelen worden getroffen om ervoor te zorgen dat er alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel dat bereikt moet worden.

Actie: Bij de inrichting van ons applicatielandschap is privacy by design de norm. Privacy by default is een thema waar organisaties nog mee worstelen. Er moeten continue afspraken worden gemaakt welke gegevens minimaal noodzakelijk zijn om specifiek doel te kunnen bereiken en waar het dus minder kan in de informatie die wordt aangereikt. Afstemming met samenwerkingspartners is daarbij essentieel. Immers voor alle data die wij ongevraagd ontvangen zonder concrete doelbinding, dragen wij ook verantwoordelijkheid.

6. *Aanstellen Functionaris voor de gegevensbescherming (FG)*

Onder de AVG is het voor overheidsorganisaties verplicht om een FG aan te stellen. Deze onafhankelijke functionaris ziet er op toe dat er binnen de organisatie gehandeld wordt in lijn met de AVG. Het geven van gevraagd/ongevraagd advies, toetsen van verwerkersovereenkomsten, bevordering bewustwording medewerkers op het gebied van privacy, is daarbij een greep uit de werkzaamheden.

Actie: In onze organisatie is een FG aangesteld die is aangemeld bij de Autoriteit Persoonsgegevens. Daarmee is aan de wettelijke verplichting voldaan. De rollen in de organisatie op het gebied van privacy worden gescheiden ingevuld.
De rol van CISO (security officer) die waakt over de (beleids)maatregelen op het gebied van informatiebeveiliging is belegd bij de Informatiemanager. De rol van FG is belegd bij de Bestuurlijk-juridisch beleidsmedewerker. Beiden werken nauw samen aan continue ontwikkeling om te kunnen blijven voldoen aan de eisen die de AVG stelt.

7. *Meldplicht datalekken*

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan onze eigen registratie van datalekken die zich hebben voorgedaan. Alle datalekken moeten gedocumenteerd worden. Met deze documentatie moet de AP kunnen controleren of aan de meldplicht is voldaan.

Actie: Het protocol voor het aanmelden van datalekken is op orde. De bevoegde functionarissen om te mogen melden zijn bekend bij de Autoriteit Persoonsgegevens. Er is een sluitend systeem om ervoor te zorgen dat het aanmelden van incidenten tijdig gebeurd bij de Autoriteit.

8. *Verwerkersovereenkomsten*

Onder de AVG is het verplicht om Verwerkersovereenkomsten af te sluiten met externe partners. Deze overeenkomsten geven inzichten in de verantwoordelijkheden en afspraken rondom het verwerken van persoonsgegevens. Het scala van Verwerkers en overeenkomsten is groot. Elke organisatie wenst uiteraard een overeenkomst op maat die aansluit bij de risico's die beide partijen lopen bij het verwerken van persoonsgegevens.

Actie: Door BMC is een inventarisatie gemaakt van de bestaande Verwerkersovereenkomsten. Deze opmerkingen worden per samenwerking meegenomen bij het beoordelen van verwerkersovereenkomsten die aan ons worden voorgelegd, of door ons worden opgesteld. Welke situatie van toepassing is (beoordelen of zelf initiatief nemen) verschilt. Uitgangspunt is wel dat wij als Verantwoordelijke voor de persoonsgegevens waarover wij beschikken, ook de regie willen hebben over de verwerking ervan. Daarbij kan soms ook sprake zijn van tegengestelde belangen. Het is dan uiteindelijk aan de organisatie zelf om af te wegen in hoeverre tegemoet kan worden gekomen aan wensen van de beoogde samenwerkingspartner over de inhoud van een verwerkersovereenkomst.

9. *Leidende toezichthouder*

Dit onderdeel van de AVG is voor onze organisatie niet van toepassing. Het thema ziet op regelgeving bij organisaties die gegevensverwerkingen in meerdere EU-lidstaten uitvoeren.

Actie: Niet van toepassing op onze organisatie.

10. *Toestemming*

Voor sommige gegevensverwerkingen is toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan die toestemming. Alles wat wij binnen de gemeente doen moet berusten op een wettelijke grondslag. In het kader van vooronderzoek is veel mogelijk, echter, er zijn ook situaties denkbaar waarbij aparte toestemming om gegevens te mogen delen noodzakelijk is. Per situatie zal moeten worden beoordeeld of de wettelijke grondslag toereikend is of dat er aanvullende toestemming gevraagd moet worden aan de betrokkene(n) van wie persoonsgegevens worden verwerkt. Dit is maatwerk.

Actie: Bij alle informatie die wordt opgevraagd moet betrokkene helder zijn op welke wettelijke grondslag dit gebaseerd is. Daarnaast moet expliciet toestemming worden gevraagd als die grondslag ontoereikend is. Dit vraagt om acties op zowel het gebied van bewustwording van medewerkers en het verankeren van de toestemmingsvraag in werkprocessen. Dit is een ontwikkelpunt.

Draagvlak
Het onderwerp betreft het voldoen aan Europese regelgeving. Het draagvlak is daarmee een gegeven.

Beoogd resultaat (hoe)
De voortgang van de implementatie van de AVG vindt plaats op verschillende niveaus in de organisatie. Periodiek wordt teruggekoppeld hoe de organisatie er voor staat.

Financiële consequenties
Geen directe consequenties. Aandachtspunt is wel het indirecte gevolg van de AVG op beschikbare personele capaciteit, doordat de rollen van CISO/FG nu worden ingevuld binnen bestaande functies. De nabije toekomst zal moeten uitwijzen of de huidige personele capaciteit structureel toereikend is, om te kunnen voldoen aan alle extra taken die de AVG met zich meebrengt.

Aanpak/uitvoering
Na vaststelling stukken in het college de privacyverklaring en het privacyreglement/privacybeleid plaatsen op de website. Daarnaast de raad informeren door middel van het plaatsen van dit collegeadvies op de ingekomen stukkenlijst.

Conclusie
Ik adviseer u om in te stemmen met het vaststellen van de privacyverklaring en het privacyreglement/privacybeleid.

Communicatie
Geen aanvullende acties noodzakelijk.

Bijlage(n)
- Privacyverklaring
- Privacyreglement
- Privacybeleid