



gemeente
Barneveld

Nr. 1052157

Collegevoorstel

Onderwerp:

voorstel betreffende vaststelling privacybeleid

Gevraagde beslissing:

1. Het beleidsstuk "Privacybeleid gemeente Barneveld" vast te stellen door de burgemeester en het college van burgemeester en wethouders, ieder voor zover het hun bevoegdheid betreft en op 1 oktober 2017 inwerking laten treden.

Raad

☒ Ter kennisname naar de raad

Nummer beleidsproduct:

☐ Op overzicht Bestaand beleid (website)

Datum 7 augustus 2017

Steller: S. Groothedde

Afd: BD-JZ

Aantal bijlagen 1

Afd.hoofd:

Bert
Komdeur

Portefeuillehouder

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 G.J. van den Hengel			
Wethouder D. J. Dorrestijn-Taal			

26 SEP. 2017

Beslissing burgemeester en wethouders :

Nummer op besluitenlijst:

39105

Gefirm. advies
thuis. van de gemeenteraad

39105

1. Inleiding

Op 25 mei treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Op deze datum dienen alle overheden en bedrijven die op grote schaal persoonsgegevens verwerken te voldoen aan deze nieuwe wet. De AVG stelt nieuwe en zwaardere eisen dan de huidige wet, de Wet bescherming persoonsgegevens. Bovendien is het de verwachting dat de slagkracht van de Autoriteit Persoonsgegevens (toezichthouder) toeneemt door een forse uitbreiding in formatie.

In de collegevergadering van 27 juni 2017 heeft uw college aangegeven dat het noodzakelijk is dat ook binnen de gemeente Barneveld voldoende aandacht is voor de onderwerpen privacy en informatiebeveiliging. Tevens is door uw college uitgesproken dat het belangrijk is dat de wet- en regelgeving ten aanzien van deze onderwerpen wordt nageleefd en naleving ook in de toekomst is geborgd.

2. Beoogd effect

Meetbaar effect: Met de vaststelling van dit privacybeleid wordt naleving van de AVG door de gemeente Barneveld vereenvoudigd en beschikt de gemeente Barneveld over een toegankelijk document waarin de belangrijkste verplichten op een heldere wijze zijn opgenomen. Hierdoor weet de gemeentelijke organisatie op welke wijze met persoonsgegevens moet worden omgegaan en welke procedure gevolgd moet worden in geval een beveiligingsincident zich heeft voorgedaan en/of persoonsgegevens zijn gelekt.

Tevens vormt een gedegen privacybeleid voor de Autoriteit Persoonsgegevens een belangrijke aanwijzing dat het onderwerp privacy op de gemeentelijke agenda staat en dat de gemeente Barneveld zich inspant om de AVG na te leven.

Maatschappelijk effect: Het privacybeleid ondersteunt de organisatie in het naleven van de AVG. Hierdoor zijn de persoonsgegevens van burgers beter beschermd. Verder is de gemeente met dit privacybeleid transparant richting burgers over de manier waarop de gemeente omgaat met persoonsgegevens. Dit kan het vertrouwen van de burger in de gemeente versterken.

3. Argumenten

Implementatie AVG en naleving

De vaststelling van het privacybeleid vormt een belangrijke stap in de implementatie van de AVG. Verder stimuleert het privacybeleid de naleving van de privacywetgeving. Dit document is namelijk toegankelijk geschreven, waardoor het voor de organisatie goed raadpleegbaar is. Verbeterde naleving van de AVG draagt direct bij aan een betere beveiliging van persoonsgegevens.

Toezicht op naleving

De AVG vereist dat een Functionaris voor de Gegevensbescherming (FG) wordt ingesteld om de organisatie te controleren op naleving van de AVG. Het privacybeleid beschrijft de taken en bevoegdheden van de FG.

Rechten burgers

De AVG breidt de rechten van burgers uit. Het privacybeleid regelt de wijze waarop burgers hun rechten kunnen uitoefenen.

Procedure meldplicht datalekken

In het geval mogelijk een datalek heeft plaatsgevonden, moet direct het protocol 'Procedure afwikkeling datalek' in werking treden. Daarin staan precies de stappen beschreven wat moet gebeuren en wie moet worden ingelicht. Deze beschreven procedure draagt bij aan een efficiënte afhandeling van een datalek, waarbij alle betrokken en verantwoordelijke partijen tijdig worden geïnformeerd. Op deze manier kan escalatie van een datalek worden voorkomen en tijdig maatregelen worden getroffen.

4. Kanttekeningen

Weinig beleidsvrijheid

De AVG is een verstrekkende en gedetailleerde wet, waardoor er weinig beleidsvrijheid is. Met dit privacybeleid is beoogd om op een praktische wijze handen en voeten te geven aan deze wet. Daarbij is waar mogelijk gekozen voor de meest effectieve en efficiënte werkwijze.

Gedragsverandering

Voor de naleving van de AVG is gedragsverandering van elke medewerker noodzakelijk. Daarom is het essentieel dat organisatiebreed er blijvende aandacht is voor 1) privacy, 2) informatiebeveiliging en 3) de procedure omtrent een datalek.

5. Financiën

In de Kadernota 2018-2020 zijn de middelen beraamd voor de functies van FG en Privacy Officer (PO). Tevens zijn deze functies opgenomen in de begroting 2018. Na goedkeuring van de begroting 2018 door de gemeenteraad zal de functie van PO intern worden ingevuld. De functie van FG zal gedeeld worden met andere gemeenten.

6. Uitvoering

Planning: De inwerkingtreding staat gepland op 1 oktober 2017.

Communicatie: Via de volgende kanalen zal intern aandacht besteed worden aan de vaststelling van het privacybeleid:

- Intranet;
- E-mail aan teamleiders en afdelingshoofden
- Aankondiging vaststelling privacy in bijeenkomst voor teamleiders.

Extern: Gemeenteblad

Implementatie: De PO en de FG zijn verantwoordelijk voor de implementatie van de AVG en dit privacybeleid. De gemeente heeft hiervoor tot 25 mei 2018 de tijd. De PO maakt deel uit van het team Juridische Zaken, afdeling B&D. De FG wordt indien mogelijk met andere gemeenten gedeeld, waardoor deze functie om meer afstand staat van de gemeente. Hierdoor kan de FG beter zijn toezichthoudende taak vervullen.

Evaluatie/controle:

- FG houdt toezicht op de naleving van o.a. het privacybeleid en rapporteert hierover aan uw college;
- Vanaf 2018 moet in de programmabegroting een passage worden opgenomen over de uitvoering en realisatie van het privacybeleid.

7. Bijlagen

1. Privacybeleid gemeente Barneveld.

Inhoudsopgave

I	Inleiding
II	Definities
III	Ingangsdatum
IV	Reikwijdte
V	Uitgangspunten
VI	Wetgeving
VII	Verantwoording
VIII	Functionaris Gegevensbescherming, Privacy Officer, Chief Information Security Officer
IX	Werkwijze
X	Meldplicht datalekken
XI	Verwerkersovereenkomst
XII	Informatiebeveiliging
XIII	Transparantie en communicatie
XIV	Cameratoezicht
XV	Afsluiting

Lijst met frequent gebruikte afkortingen

FG:	Functionaris voor de Gegevensbescherming
PO:	Privacy Officer
CISO:	Chief Information Security Officer
AP:	Autoriteit Persoonsgegevens
Wbp:	Wet bescherming persoonsgegevens
AVG:	Algemene verordening gegevensbescherming
Awb:	Algemene wet bestuursrecht

Privacybeleid gemeente Barneveld

I Inleiding

In de maatschappij is privacy een onderwerp dat veel in de belangstelling staat. Daarnaast is het informatie- en privacyrecht volop in ontwikkeling.

Gegevensbescherming en het verwerken van privacygevoelige informatie is ook een relevant onderwerp voor de gemeente Barneveld. De gemeente verzamelt en bewerkt namelijk veel persoonsgegevens voor de dienstverlening aan inwoners en bedrijven. Bij gegevensbescherming gaat het om het zorgvuldig, veilig en doelmatig verwerken van persoonsgegevens. Het verwerken van persoonsgegevens omvat alle handelingen die met persoonsgegevens uitgevoerd kunnen worden zoals het verzamelen, vastleggen, bewaren, wijzigen, opvragen, gebruiken en inzien. Persoonsgegevens zijn de gegevens over een geïdentificeerde persoon of gegevens waarmee een persoon geïdentificeerd kan worden. Hierbij kan gedacht worden aan een naam, adresgegevens, foto of een e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn, zoals een kentekenplaat op een voertuig of een IP-adres. Bijzondere persoonsgegevens zijn persoonsgegevens die extra gevoelig zijn, zoals het BSN en informatie over iemands gezondheid of financiële situatie. Privacy is samenvattend te omschrijven als respect voor de persoonlijke levenssfeer van een individu. Om te voorkomen dat een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer, is onder meer bij wet voorzien in waarborgen.

De gemeente Barneveld hecht veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Binnen de gemeente is hiervoor al veel aandacht. Om de positie van het privacyvraagstuk verder te versterken heeft het college van burgemeester en wethouders besloten dat privacybeleid wenselijk is. Dit privacybeleid is praktisch ingestoken en vormt een aanvulling op de verplichtingen die voortvloeien uit Wet bescherming persoonsgegevens en de Europese Algemene verordening gegevensbescherming. De Algemene wet gegevensbescherming is vanaf 25 mei 2018 van toepassing. Tot deze datum heeft gemeente Barneveld de tijd om de Europese verordening en dit privacybeleid te implementeren.

In dit beleid staan kaders beschreven voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en de omgang met deze gegevens. De kaders gelden voor de gemeente, samenwerkingsverbanden die zijn of worden aangegaan en derden die zijn of worden ingeschakeld. Verder kan het beschermen van persoonsgegevens niet geborgd worden zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom ook samen met het Informatiebeveiligingsbeleid.

II Definities

Persoonsgegeven: elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat deze informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Bijzonder persoonsgegevens: Elk gegeven over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond, strafrechtelijk verleden en het Burgerservicenummer (BSN).

Verwerken: alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen.

Verwerkingsverantwoordelijke: De verwerkingsverantwoordelijke is een persoon of een organisatie die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt.

Verwerker: De verwerker is een persoon of organisatie aan wie de verwerkingsverantwoordelijke de verwerking van persoonsgegevens heeft uitbesteed.

Datalek: Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking.

III Ingangsdatum

Het "Privacybeleid gemeente Barneveld" is in werking getreden op 1 oktober 2017.

IV Reikwijdte

Dit gemeentelijk privacy beleid is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden.

V Uitgangspunten

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding

De gemeente zorgt ervoor dat persoonsgegevens alleen voor uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Dataminimalisatie

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij een wettelijke grondslag aanwezig is om op dit verbod een uitzondering te maken.

Integriteit, vertrouwelijkheid en informatiebeveiliging

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Rechten van betrokkenen

De gemeente honoreert alle rechten die betrokkenen onder de Algemene Verordening Gegevensbescherming hebben. Betrokkenen hebben op grond van deze wet onder andere de volgende rechten:

- Recht op informatie;
- Recht op inzage;
- Recht op rectificatie;
- Recht op verwijdering van persoonsgegevens;
- Recht op beperking van de verwerking;
- Het recht op overdraagbaarheid van persoonsgegevens;
- Recht op bezwaar.

Klachten

Betrokkenen kunnen klachten over de verwerking van persoonsgegevens op een laagdrempelige wijze indienen en deze klachten worden op een voortvarende manier afgehandeld.

Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling en de beveiliging aan moet voldoen. Door deze afspraken wordt geborgd dat ook derden op een integere en vertrouwelijke manier omgaan met de verwerking van persoonsgegevens waarvoor de gemeente verantwoordelijk is.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichten te kunnen naleven.

Ondersteuning medewerkers

Om de medewerkers te instrueren in het omgaan met en verwerken van persoonsgegevens, stelt de gemeente procedures en werkinstructies beschikbaar voor haar medewerkers. Tevens wordt voldoende aandacht besteed aan de bewustwording van medewerkers en wordt voorzien in adequate (juridische) ondersteuning.

VI Wetgeving

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat er onnodige of te vergaande inbreuken worden gemaakt. De Wet bescherming persoonsgegevens (Wbp) biedt hiervoor het wettelijk kader. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Verder zal ook de Uitvoeringswet Algemene Verordening Gegevensbescherming worden vastgesteld en in werking treden.

De AVG bouwt voort op de Wbp en zorgt onder andere voor versterking en uitbreiding van de privacyrechten van betrokkenen en meer verantwoordelijkheden voor de gemeente Barneveld. Met de naleving van het privacybeleid spant de gemeente Barneveld zich in om aan de AVG te voldoen.

In dit privacybeleid zijn de in de AVG opgenomen definities integraal van toepassing.

VII Verantwoording

Verwerkingsverantwoordelijke

De verantwoordelijke voor de verwerking van persoonsgegevens is het college van burgemeester en wethouders (college) en/of de burgemeester. Welk bestuursorgaan verantwoordelijk is, is afhankelijk van hetgeen waarop de verwerking van persoonsgegevens betrekking heeft. Zo is de burgemeester als bestuursorgaan verantwoordelijk voor de verwerking van persoonsgegevens wanneer dit ziet op situaties die vallen onder openbare en veiligheid.

De wethouder met de portefeuille 'Bedrijfsvoering' (portefeuillehouder) is voor incidenten dan wel vraagstukken omtrent dit privacybeleid het eerste aanspreekpunt.

In verband met de leesbaarheid van het privacybeleid wordt hierna alleen het college benoemd waar beide bestuursorganen worden bedoeld.

Verantwoording aan de gemeenteraad

Het college legt verantwoording af aan de gemeenteraad over de uitvoering en realisatie van beleid. Met ingang van 2018 neemt het college in de programmabegroting een passage op over de uitvoering en realisatie van het privacybeleid. Naast de jaarlijkse verantwoording in de

programmabegroting heeft het college de algemene informatieplicht om de gemeenteraad te informeren over bijzonderheden.

Verantwoording en uitvoering

De eindverantwoordelijkheid voor de ambtelijke uitvoering van het privacybeleid ligt bij de directie van de gemeente. De directie rapporteert door middel van een periodieke kennisgeving aan de portefeuillehouder. Elk afdelingshoofd is binnen zijn afdeling verantwoordelijk voor de naleving van het privacybeleid en een zorgvuldige verwerking van persoonsgegevens.

Vastlegging privacybeleid

Het college stelt het gemeentelijk privacybeleid vast. Bij de vaststelling dan wel herziening van het privacybeleid zal het college de aanbevelingen van de Functionaris Gegevensbescherming in acht nemen.

VIII Functionaris Gegevensbescherming , Privacy Officer, Chief Information Security Officer

Functionaris voor de Gegevensbescherming

De functie van FG is wettelijk verplicht. De FG ziet toe op naleving van de privacywetgeving en het privacybeleid binnen de gemeente. Hiervoor is het noodzakelijk dat de FG zijn taken en plichten onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitoefening van zijn functie. De werkzaamheden die de FG uitvoert hebben een wettelijke grondslag.

Taken:

- Informeren en adviseren van de organisatie en verwerkers over hun verplichtingen die zij hebben op grond van de AVG en overige regelgeving op het gebied van privacy en persoonsgegevens;
- Advisering van het college;
- Toezien op naleving van AVG en overige regelgeving op het gebied van privacy en persoonsgegevens;
- Toezien op naleving van het privacybeleid;
- Rapporteren van bevindingen aan het college en directie;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van medewerkers;
- Advisering met betrekking tot de gegevensbeschermingseffectbeoordeling, toezien op de uitvoering daarvan en adviseren over noodzakelijke vervolgacties;
- Bijhouden register verwerkingsactiviteiten;
- Advisering van de PO en CISO bij de afhandeling van beveiligingsincidenten;
- Advisering van de PO bij de afhandeling van ingewikkelde klachten;
- Samenwerken met de Autoriteit Persoonsgegevens (AP);
- Optreden als contactpunt voor de AP;
- Ontwikkelen van professionele kwaliteit en deskundigheid.

De taken zoals hierboven uitgewerkt moeten bij de FG moeten worden belegd. Een aantal taken kunnen echter ook in (nauwe) samenwerking met of door de PO en CISO worden uitgevoerd. Hierover zullen werkafspraken worden gemaakt. De FG blijft niettemin eindverantwoordelijke.

De FG heeft controlebevoegdheden tot zijn beschikking zoals beschreven in titel 5.2 van de Algemene wet bestuursrecht (Awb). Deze bevoegdheden zijn noodzakelijk voor de uitoefening van geloofwaardig en effectief toezicht. Tevens gelden ook de waarborgen en beperkingen zoals beschreven in titel 5.2 Awb. De belangrijkste bevoegdheden zijn voor de FG hieronder nader uitgewerkt.

Wettelijke bevoegdheden:

Betreden van ruimten: Indien het noodzakelijk is voor de uitvoering van bovengenoemde taken is de FG bevoegd om ongevraagd alle ruimten te betreden, voor zover die ruimten vallen onder de reikwijdte van het aan de FG wettelijk opgedragen toezicht.

Vragen van inlichtingen: De FG verkrijgt alle inlichtingen die noodzakelijk zijn voor de uitvoering van bovengenoemde taken. De verwerkingsverantwoordelijke verleent alle medewerking om deze inlichtingen binnen een redelijke termijn te verstrekken. Geen medewerking hoeft te worden verleend in het geval de verwerkingsverantwoordelijke of diens ondergeschikte uit hoofde van het ambt, beroep of wettelijk voorschrift is verplicht tot geheimhouding.

Vragen om inzage: De FG is bevoegd om inzage te vragen van zakelijke gegevens en bescheiden. Hiervan mag de FG tevens kopieën maken. Het gaat hierbij niet alleen om fotokopieën, maar ook van kopieën van (gedeelten van) geautomatiseerde gegevensbestanden. De verwerkingsverantwoordelijke moet hieraan meewerken, tenzij de verwerkingsverantwoordelijke of diens ondergeschikte uit hoofde van het ambt, beroep of wettelijk voorschrift is verplicht tot geheimhouding.

Onderzoeken van zaken: Voor de uitvoering van bovengenoemde taken kan het betreden van ruimten soms niet voldoende zijn om toezicht uit te oefenen. Indien noodzakelijk verkrijgt de FG daarom toegang tot (computer-)systemen waarin persoonsgegevens worden verwerkt. De FG zal desnoods de beschikking dienen te krijgen over de relevante inloggegevens. Tevens zal de FG op de hoogte dienen te zijn hoe, na het inloggen, de relevante bestanden kunnen worden bevraagd.

Contact: De FG is te bereiken via: fg@barneveld.nl.

Privacy Officer

De PO heeft een brede functie, waarbij de PO hoofdzakelijk dient als interne (juridische) ondersteuning van de gehele organisatie voor alle privacy gerelateerde vraagstukken en dilemma's.

Taken:

- Ondersteuning bieden aan de FG;
- Implementeren privacyregelgeving en privacybeleid in de organisatie;
- Zorgdragen voor kennisoverdracht en bewustwording in de gemeente;

- Functioneren als (juridische) vraagbaak voor de organisatie;
- Advisering bij gegevensuitwisseling met derden;
- Uitvoeren van gegevensbeschermingseffectbeoordelingen;
- Afhandeling van datalekken en het beheren van het register waarin datalekken worden geregistreerd. Afhankelijk voor de aard en de impact van een datalek worden de FG en CISO ook betrokken bij de afhandeling daarvan. De PO mag correctieve en/of preventieve maatregelen nemen. Over de getroffen dan wel de te nemen maatregelen moet de portefeuillehouder, de FG en de CISO zo spoedig mogelijk geïnformeerd worden.
- Afhandeling van klachten met betrekking tot de verwerking van persoonsgegevens;
- Afhandeling van verzoeken van betrokkenen, zoals recht op informatie, rectificatie en recht van bezwaar;
- Het ontwikkelen van professionele kwaliteit en deskundigheid.

Contact: De PO is te bereiken via: privacy@barneveld.nl.

Chief Information Security Officer

Persoonsgegevens kunnen niet geborgd worden zonder adequate informatiebeveiliging. De CISO draagt zorg voor de informatiebeveiliging. De werkzaamheden die de CISO uitvoert worden beschreven in het Informatiebeveiligingsbeleid. De CISO stuurt op en evalueert de naleving van het Informatiebeveiligingsplan. Concreet adviseert de CISO het management over beveiliging, mogelijke risico's en de daarbij behorende mitigerende maatregelen. Dit zijn alle maatregelen die negatieve effecten van het besluit of handelen voorkomen of beperken. Tevens is de CISO betrokken bij de afhandeling van een datalek. De CISO mag correctieve en/of preventieve maatregelen nemen. Over de getroffen dan wel de te nemen maatregelen moet de portefeuillehouder, de FG en de PO zo spoedig mogelijk geïnformeerd worden.

IX Werkwijze

Verwerking

Op de verwerking van persoonsgegevens is de AVG van toepassing. De verwerking van persoonsgegevens is elke (geautomatiseerde) handeling met persoonsgegeven(s).

Verwerking wordt als volgt omschreven:

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Kortom, uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doeleinden

Volgens de AVG mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. Soms is het doel omschreven in de wet. De gegevens mogen niet voor andere doelen verwerkt worden.

Rechtmatige grondslag

De AVG zegt dat voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- Voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
- Om een wettelijke verplichting na te komen;
- Om de vitale belangen van de betrokkene te beschermen;
- Voor de goede vervulling van een taak van algemeen belang of een aan de gemeente opgedragen taak.

Wijze van verwerking

Bij de verwerking van persoonsgegevens gelden een aantal spelregels:

- De verwerking moet in overeenstemming zijn met de wet;
- De verwerking moet zorgvuldig gebeuren;
- De persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf;
- Persoonsgegevens worden alleen verzameld als het doel niet op een andere manier kan worden bereikt;
- Het verzamelen van persoonsgegevens staat in verhouding tot het doel. Er wordt dus niet meer gevraagd dan nodig;
- Persoonsgegevens worden alleen verwerkt door personen met een geheimhoudingsplicht;
- Op de verwerking van persoonsgegevens is tevens het Informatiebeveiligingsbeleid van toepassing.

Doorgifte

De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

Bewaren en vernietiging persoonsgegevens

Op grond van de AVG gelden geen concrete bewaartermijnen. Daarom wordt het uitgangspunt gehanteerd dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking of zoals vastgelegd in de Archiefwet. In het geval in bijzondere wetten concrete bewaartermijnen zijn opgenomen, dan zijn deze termijnen leidend. Wanneer persoonsgegevens niet langer bewaard (mogen) worden, worden deze gegevens vernietigd of aangepast zodat daarmee personen niet langer geïdentificeerd kunnen worden.

Register van verwerkingen

De gemeente houdt een register bij met daarin een overzicht van alle verwerkingen van persoonsgegevens waarvoor de gemeente verwerkingsverantwoordelijke is.

Gegevensbeschermingsbeoordeling

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens wordt een gegevensbeschermingseffectbeoordeling uitgevoerd voor verwerkingen die waarschijnlijk een verhoogt risico opleveren voor betrokkenen. Deze beoordeling zorgt ervoor dat alle risico's van een verwerking (vroegtijdig) in kaart worden gebracht en maatregelen kunnen worden getroffen.

Bewustwording

Het is belangrijk dat medewerkers bewust met persoonsgegevens omgaan. Om bewustwording te realiseren is kennisoverdracht nodig. De FG, PO en CISO zorgen ervoor dat informatie over gegevensbescherming en informatiebeveiliging herhaaldelijk onder de aandacht wordt gebracht van de gehele organisatie.

X Meldplicht datalekken

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een datalek hebben ontdekt, tenzij het niet waarschijnlijk is dat het datalek een risico vormt voor de betrokkene. Soms moet dit lek ook worden gemeld aan de personen van wie de gegevens zijn gelekt.

Om in het geval van een datalek snel en daadkrachtig te kunnen handelen is een procedure ingericht die inwerking treedt bij aanmelding van een datalek. De beoordeling van een gemeld lek vindt plaats door de PO, CISO en indien nodig de FG. Een datalek wordt vertrouwelijk behandeld. Bij een datalek die wordt gemeld bij de Autoriteit Persoonsgegevens worden tevens de portefeuillehouder, de directie en het betrokken afdelingshoofd geïnformeerd. Deze kennisgeving gebeurt geanonimiseerd, tenzij dit omwille van de afhandeling van het datalek niet mogelijk is.

De portefeuillehouder, directie en betrokken afdelingshoofd worden ook geïnformeerd indien de omstandigheden omtrent een datalek daartoe aanleiding geven. Het college wordt altijd geïnformeerd als dat gelet op de aard of omvang van een datalek noodzakelijk is.

Een datalek kan gemeld worden via datalek@barneveld.nl.

XI Verwerkersovereenkomst

Bij veel gemeentelijke processen worden persoonsgegevens verwerkt door derden. Om een correcte en veilige omgang met persoonsgegevens door derden te kunnen borgen, zal de gemeente waar nodig de eisen rondom gegevensverwerking borgen in een verwerkersovereenkomst. Het afdelingshoofd of teamleider die een dergelijke uitbesteding, samenwerking of uitwisseling aangaat, ziet toe op de totstandkoming van deze afspraken. De volgende onderdelen maken in ieder geval deel uit van een verwerkersovereenkomst:

- Een overzicht van de te verwerken persoonsgegevens;
- Een beschrijving van de type verwerkingen;
- Een overzicht van de te treffen beveiligingsmaatregelen;
- Een beschrijving van de procedure in geval van een datalek zich voordoet.

De gemeente beschikt over een registratie van verwerkersovereenkomsten.

XII Informatiebeveiliging

De gemeente Barneveld is sinds 2013 bezig met de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De BIG is een zelfreguleringsinstrument en bestaat uit een set van beveiligingsmaatregelen, inclusief maatregelen die zien op de fysieke beveiliging. Verder heeft de gemeente Barneveld ingestemd met de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'.

De gemeente Barneveld heeft in 2013 het Informatiebeveiligingsbeleid vastgesteld. Dit beleid wordt iedere drie jaar geëvalueerd en zo nodig herzien. In het geval (beveiliging)situaties daartoe aanleiding geven, kan het Informatiebeveiligingsbeleid ook eerder aangepast worden.

Naast het informatiebeveiligingsbeleid, stelt de gemeente Barneveld elk jaar een informatiebeveiligingsplan op. Het Informatiebeveiligingsplan vormt een uitwerking van het informatiebeveiligingsbeleid, waarmee per jaar de te nemen maatregelen worden vastgesteld. Verder worden in het Informatiebeveiligingsplan acties beschreven om de reeds geïmplementeerde maatregelen te waarborgen en te controleren op volledigheid en/of toepasbaarheid (Plan-, Do-, Check-, Act-cyclus). Daarnaast geldt het verantwoordingsnormenkader Eenduidige Normatiek Single Information Audit (ENSIA).

XIII Transparantie en communicatie

Wet openbaarheid van bestuur (Wob)

Via de Wob kan een verzoek worden ingediend bij de gemeente. Bij een dergelijk verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie (Who)

De Who regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Informatieplicht

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens en hun rechten onder de AVG. Deze informatie is te vinden op de website van de gemeente Barneveld.

Indienen van een verzoek

Wanneer een betrokkene gebruik wenst te maken van zijn rechten onder de AVG kan de betrokkene bij een verzoek indienen. Dit verzoek kan schriftelijk, per e-mail of via de website van de gemeente worden ingediend. De verzoeker om informatie moet zich altijd identificeren. De informatie waarom wordt verzocht wordt kosteloos verstrekt, tenzij het verzoek buitensporig is.

Na ontvangst van een verzoek ontvangt betrokkene binnen vier weken een besluit en de informatie waarom is verzocht. Deze termijn kan met acht weken worden verlengd. Een verzoek kan worden geweigerd als het verzoek ofwel kennelijk ongegrond is ofwel buitensporig is.

Tegen het besluit kan betrokkene bezwaar maken of een klacht indienen bij de Autoriteit Persoonsgegevens.

Contact

Vragen met betrekking tot privacy, het privacybeleid of de overige wet- en regelgeving op het gebied van privacy kunnen gericht worden aan de Privacy Officer van de gemeente Barneveld: privacy@barneveld.nl.

XIV Cameratoezicht

In de gemeente Barneveld is er cameratoezicht. Het cameratoezicht valt op het moment van vaststelling van dit beleid niet onder de verantwoordelijkheid van de gemeente maar onder de verantwoordelijkheid van Keurmerk Veilig Ondernemen Barneveld/Voorthuizen en Stichting Veiligheid en Beheer Bedrijventerreinen Barneveld (Stichting VBBB). Op dit moment doen zich in de gemeente namelijk geen openbare orde problemen voor die de inzet van structureel cameratoezicht rechtvaardigt. KVO en Stichting VBBB zetten cameratoezicht in met als doel om personen, gebouwen, terreinen, zaken en productieprocessen in winkelgebieden en de bedrijventerreinen te beveiligen. Hiervoor moeten KVO en Stichting VBBB als verantwoordelijke aantonen te voldoen aan alle wet- en regelgeving, met name op het gebied van de beveiliging van persoonsgegevens.

XV Afsluiting

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

DISCLAIMER

Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.