gemeente Berkelland

GEMEENTEBLAD

Officiële uitgave van de gemeente Berkelland

Nr. 280462

27 december 2018

Besluit van het college van burgemeester en wethouders van de gemeente Berkelland houdende regels omtrent privacy Privacy beleid Gemeente Berkelland

1 Inleiding

De gemeente Berkelland heeft persoonsgegevens nodig om haar taken uit te kunnen voeren. Zonder de verwerking van persoonsgegevens is het onmogelijk om bijvoorbeeld aan een inwoner een paspoort te verstrekken of een vergunning te verlenen. De inwoner moet er hierbij op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met persoonsgegevens omgaat.

De gemeente verzamelt voor de uitvoering van haar taken persoonsgegevens en slaat deze op voor de dienstverlening aan burgers, bedrijven en instellingen. Hierbij kan het gaan om de gegevens in de gemeentelijke basisregistratie personen, de registratie van bijstandsgerechtigden, het bijhouden van gegevens voor bouwaanvragen en het bijhouden van gegevens van mensen met een Wmo- of jeugdhulpvoorziening. De gemeente Berkelland werkt daarnaast samen met een breed scala aan partners in het maatschappelijke veld en deelt daarin, waar dit nodig is voor de uitoefening van haar taak, ook persoonsgegevens.

Uit onder meer publicaties van de Autoriteit Persoonsgegevens en de regelmaat waarin het onderwerp aandacht krijgt in de media blijkt dat het verwerken van persoonsgegevens zorgvuldig moet gebeuren. Het niet adequaat verwerken van persoonsgegevens kan zelfs leiden tot onacceptabele situaties. Bijvoorbeeld als iemands identiteit wordt ‘gestolen’ en vervolgens wordt misbruikt.
Een juiste toepassing van de wettelijke regels acht het college van burgemeester en wethouders dan ook van groot belang.

De gemeente heeft de taak om er voor te zorgen dat de personen over wie de gemeente gegevens bijhoudt (of laat bijhouden), op een passende manier beschermd worden tegen de risico’s van de informatiemaatschappij. Dit privacy beleid vormt een nadere uitwerking van de wettelijke regelgeving. Het college streeft een zorgvuldige verwerking van persoonsgegevens na. Het beschermen van persoonsgegevens kan overigens niet geborgd worden zonder adequate informatiebeveiliging. Het privacy beleid hangt daarom ook nauw samen met het informatiebeveiligingsbeleid van de gemeente Berkelland, waarin de gemeente het geheel van technische- en organisatorische maatregelen beschrijft en daarmee ook invulling geeft aan de beveiliging van informatie en persoonsgegevens.

2 Visie en doelstelling bescherming van persoonsgegevens

Dit privacy beleid verwoordt de bestuurlijke visie van het college van burgemeester en wethouders van Berkelland op privacy zoals deze besloten ligt in de Europese en Nederlandse privacywetgeving.

2.1 Visie

De gemeente Berkelland respecteert de privacy van natuurlijke personen, zoals inwoners, ondernemers en medewerkers, en zorgt, door het zorgvuldig omgaan met persoonsgegevens, voor maatschappelijk vertrouwen en draagvlak.

2.2 Doelstelling

Dit privacy beleid, geeft handvatten voor het beantwoorden van vragen op het gebied van privacy. Er wordt onder meer aandacht besteed aan:

- het verwerken van persoonsgegevens in het algemeen, waaronder het borgen van een zorgvuldige verwerking;
- hoe te handelen als de privacy wordt geschonden en;
- de rechten van burgers/inwoners en medewerkers.

Privacy beleid is niet zozeer een extra last; het biedt ook voordelen. Door de bescherming van de persoonsgegevens te borgen in de werkprocessen:

- beschermt het college zijn inwoners tegen risico's van de informatiemaatschappij;
- beheerst het college gemeentelijke afbreuk- en aansprakelijkheidsrisico's;
- bevordert het college de kwaliteit, continuïteit, veiligheid en klantgerichtheid van de gemeentelijke administratieve organisatie;
- bouwt het college aan maatschappelijk vertrouwen en draagvlak;
- respecteert de gemeente Berkelland de privacy;
- kan het college met vertrouwen verantwoording afleggen aan de raad en, in voorkomende gevallen, de Autoriteit Persoonsgegevens of de rechter.

2.3 Reikwijdte

Dit privacy beleid is van toepassing op alle verwerkingen van persoonsgegevens waarvoor de gemeente verantwoordelijk is in de zin van de Europese Algemene verordening gegevensbescherming en aanverwante wet- en regelgeving. Dit beleid is dan ook bedoeld als handvat voor de burger om de gemeente te kunnen volgen en aanspreken op het zorgvuldig omgaan met persoonsgegevens.

3 Juridisch kader

Dit beleid regelt de nadere uitwerking van de Algemene verordening gegevensbescherming (hierna ook: de AVG). De in de AVG opgenomen definities en overige normen zijn onverkort van toepassing. Gegevensbescherming kan alleen gerealiseerd worden door het borgen van informatieveiligheid. Voor informatieveiligheid streeft de gemeente er naar te voldoen aan de kaders van de Strategische en Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (de zogeheten BIG). Naast de AVG bevat een groot aantal andere wetten specifieke vereisten voor gegevensverwerking. Denk hierbij onder andere aan:

- de Wet Basisregistratie Personen (Wet BRP, deze wet vormt de grondslag voor de basisregistratie van persoonsgegevens)
- de Wet politiegegevens,
- de Wet justitiële en strafvorderlijke gegevens,
- de Archiefwet (bewaartermijnen),
- de Telecommunicatiewet,
- de Wet Maatschappelijke Ondersteuning (WMO),
- de Jeugdwet.

4 Governance en organisatorische borging gegevensverwerking

4.1 Verantwoordelijke

Het college van burgemeester en wethouders, de burgemeester en de gemeenteraad zijn de verantwoordelijke voor verwerking van persoonsgegevens, zoals bedoeld in de AVG.

4.2 Verantwoordelijkheid voor uitvoering van beleid

De verantwoordelijkheid voor de uitvoering van beleid ligt bij de gemeentesecretaris. Aan deze verantwoordelijkheid geeft hij mede invulling door zorg te dragen voor voldoende kennis en bewustzijn van zorgvuldige verwerking van persoonsgegevens bij alle betrokken medewerkers.
De gemeentesecretaris stelt tevens de procedures vast waarin de werkwijze ten aanzien van de verwerking van persoonsgegevens is geregeld.

4.3 Functionaris gegevensbescherming (FG)

Het gemeentebestuur benoemt een Functionaris Gegevensbescherming (hierna ook: FG), zoals bedoeld in de artikelen 37, 38 en 39 AVG. De FG is belast met het toezicht op de uitvoering van het privacy beleid van de gemeente.

4.4 De Chief Information Security Officer (CISO)

De Chief Information Security Officer (hierna ook: CISO) coördineert de informatiebeveiliging. De CISO is belast met het toezicht op de betrouwbaarheid van de informatievoorziening en rapporteert hierover aan de directie en het college van burgemeester en wethouders. De uitvoerende taken zijn zoveel mogelijk belegd bij medewerkers in de ambtelijke organisatie voor informatiebeveiliging. De organisatie

van de informatiebeveiliging is uitgewerkt in het Informatiebeveiligingsbeleid van de gemeente Berkelland.

4.5 De coördinator privacybescherming en informatieveiligheid (coördinator P&I)
De coördinator privacybescherming en informatieveiligheid (hierna coördinator P&I) ondersteunt de FG en de CISO bij de uitvoering van hun taken.

4.6 Verantwoording aan de gemeenteraad
Net zoals het college jaarlijks aan de gemeenteraad verantwoording aflegt over de gemeentelijke uitgaven, legt het college ook jaarlijks via de P&C cyclus, aan de raad verantwoording af over de uitvoering en realisatie van het privacy beleid.
Naast deze jaarlijkse verantwoording, hebben het college en de burgemeester op grond van de artikelen 169 en 180, tweede lid van de Gemeentewet de actieve informatieplicht om de raad te informeren over bijzonderheden (incidenten) bij gegevensverwerkingen.

5 Verwerkingen van persoonsgegevens

Er zijn diverse beleidsonderwerpen waar verwerking van persoonsgegevens aan de orde is. Zonder uitputtend te willen zijn worden hier de belangrijkste beleidsvelden vermeld:
- Dienstverlening aan burgers/ inwoners, bedrijven en instellingen,
- Sociaal domein, Wet maatschappelijke ondersteuning, Jeugdwet en onderwijswetten (inclusief leerlingenvervoer)
- Ruimtelijk domein (Wet algemene bepalingen omgevingsrecht, Wet ruimtelijke ordening, Omgevingsloket),
- Verzoeken om informatie van burgers/ inwoners, bedrijven en instellingen (al dan niet gebaseerd op de Wet openbaarheid van bestuur).

5.1 Voorwaarden voor verwerking: algemene regels
Hoofdregel is dat persoonsgegevens alleen *in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt*. Dit noemen we rechtmatigheid.
Daarnaast mogen persoonsgegevens slechts verzameld worden als daarvoor een precieze doelomschrijving wordt gegeven. Bovendien bepaalt de wet dat persoonsgegevens slechts mogen worden verwerkt voor zover zij *toereikend , ter zake dienend en niet bovenmatig zijn*. Dit noemen we proportionaliteit.
De betrokkene heeft ook *recht op informatie* als er persoonsgegevens van hem worden verwerkt. Degene die persoonsgegevens vraagt moet hem onder andere laten weten wie hij is en wat voor gegevens hij waarvoor verwerkt. Dit noemen we transparantie.

Behalve bovenvermelde algemene regels geldt dat er voor elke verwerking van persoonsgegevens een grondslag aanwezig moet zijn. In het merendeel van de gevallen verstrekt de betrokkene de persoonsgegevens zelf. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd. Denk hierbij aan: persoonsgegevens, adresgegevens, bedrijfsgegevens, inkomensgegevens, gezinssamenstelling, uitkeringen, onderwijsgegevens, zorgindicaties, etc. Dit is in overeenstemming met het principe van ‘eenmalige uitvraag en meervoudig gebruik’ dat door de overheid en de gemeente wordt voorgestaan. Als voor het uitvoeren van bepaalde wettelijke taken en/ of wet- en regelgeving persoonsgegevens verwerkt moeten worden, dan worden deze gegevens opgevraagd uit de basisregistratie personen (zie artikel 1.7 Wet BRP).

Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van die specifieke taak. Gegevens worden niet zonder wettelijke grondslag gedeeld. Bijzondere gegevens worden niet verwerkt, tenzij dit nodig is voor het uitvoeren van een wettelijke taak en/ of wet- en regelgeving. Zo kunnen op grond van de Wet maatschappelijke ondersteuning en/ of Jeugdwet medische- en gezondheidsgegevens worden gebruikt bij de behandeling van een ondersteuningsverzoek of een hulpvraag.

5.2 Uitgangspunten
Het wettelijk kader, zoals hiervoor beschreven, is bepalend bij het formuleren van de uitgangspunten van beleid. Het privacy beleid is gestoeld op de volgende beleidsuitgangspunten:

- De gemeente verwerkt alleen gegevens van en over inwoners/burgers die noodzakelijk zijn voor het uitvoeren van gemeentelijke taken;
- De gemeente informeert inwoners/burgers over de verwerking van persoonsgegevens;
- De gemeente bewaart gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en vernietigt deze daarna;
- De gemeente gaat terughoudend om met informatie van en over inwoners/burgers. Medewerkers worden daarover geïnstrueerd;
- De gemeente gaat bij handhaving terughoudend om met informatie van en over inwoners/burgers;
- De gemeente deelt persoonsgegevens intern en extern alleen voor zover dat strikt noodzakelijk is voor de taakuitvoering;
- De gemeente zorgt ervoor dat persoonsgegevens niet voorkomen in openbare verslagen, als daar geen noodzaak voor is;
- Als de gemeente gegevens openbaart als gevolg van een WOB-verzoek, stelt de gemeente alles in het werk om gegevens van inwoners te anonimiseren;
- Als de gemeente zelf wettelijk gegevens openbaar moet maken, dan wordt aan betrokken inwoners/burgers eerst om toestemming voor openbaarmaking gevraagd en wordt gegevensverstrekking tot een minimum beperkt;
- Als de gemeente gegevens ter inzage legt, dan wordt van betrokken inwoners/burgers de gegevensverstrekking tot een minimum beperkt;
- De gemeente draagt zorg voor het goed uitvoeren van het privacy beleid door medewerkers en samenwerkende instanties;
- De gemeente voert toezicht uit op het privacy beleid en de uitvoering ervan;
- Hoe met privacy wordt omgegaan en hoe de privacy te allen tijde wordt geborgd, wordt op een transparante manier duidelijk gemaakt;
- Daar waar sprake is van verwerking van persoonsgegevens worden werkwijzen vastgelegd en op professionele wijze uitgevoerd conform protocollen of procesbeschrijvingen. Deze procedures worden door de directie vastgesteld;
- Afhandeling van klachten en bezwaren van inwoners/burgers, bedrijven en instellingen over privacy aspecten vindt op een toegankelijke, laagdrempelige wijze plaats;
- Bij samenwerking met externe partners, waar sprake is van verwerking van persoonsgegevens, worden er afspraken gemaakt over de voorwaarden voor een zorgvuldige verwerking en de controle daarop.

5.3 Privacy Impact assessment (PIA)

Op het moment dat er sprake is van een verhoogd risico bij het gebruik van persoonsgegevens, worden de privacy risico's in kaart gebracht door een Privacy Impact Assessment (PIA). Door middel van een PIA zal moeten worden aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd. Pas nadat de PIA is uitgevoerd en de maatregelen zijn getroffen die nodig zijn om de risico's te beperken, verwerkt de gemeente de persoonsgegevens. In geval van het verwerken van bijzondere persoonsgegevens en profilering wordt altijd een PIA uitgevoerd.
Over de inhoud van de PIA worden de FG en de CISO om advies gevraagd.

5.4 Datalek

De gemeente gaat zorgvuldig om met persoonsgegevens. Toch kan het voorkomen dat onbevoegde personen toegang krijgen tot persoonsgegevens, of persoonsgegevens kwijt zijn geraakt. In dat geval spreken we van een datalek. Wanneer er een datalek is vastgesteld, wordt direct actie ondernomen aan de hand van het protocol datalekken. De afhandeling van het datalek is de verantwoordelijkheid van de FG. De FG houdt een logboek bij waarin datalekken zijn opgenomen.

5.5 Privacy by design

Door het borgen van de privacyaspecten aan het begin van het inkoop, ontwikkel- en inrichtingsproces wordt ervoor gezorgd dat inbreuk op de privacy van de betrokkenen zo veel mogelijk wordt beperkt. Met name bij de aanschaf, ontwikkeling en inrichting van ICT (infrastructuur) en/of applicaties moet hier aandacht voor zijn.
Onder privacy by design maatregelen verstaan wij onder meer het afsluiten van verwerkersovereenkomsten, toegangsbeveiliging, encryptie, verwijderen van persoonsgegevens en dataminimalisatie. Het nadenken over privacy by design is van groot belang om het voldoen aan de normen op het gebied van privacy te borgen.

5.6 Privacy by default

Aanvullend op privacy by design wordt als uitgangspunt gehanteerd dat de instellingen van een programma, app, website of dienst zodanig zijn dat maximale privacy wordt betracht. Het gaat daarbij niet alleen om opties die kunnen worden ingesteld.

6 Functionaris Gegevensbescherming

6.1 Toezicht

Voor de uitoefening van zijn toezichthoudende functie beschikt de FG over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn.

- Het betreffende bestuursorgaan en de personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken de FG desgevraagd alle inlichtingen en verlenen de FG alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.
- De FG heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt.
- De FG is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.
- De FG rapporteert over zijn bevindingen aan het college van burgemeester en wethouders. Hij geeft aanbevelingen over te nemen maatregelen, die een goede werking van de verwerking van persoonsgegevens moeten helpen waarborgen.
- De FG kan niet ontslagen worden of een sanctie krijgen als gevolg van de uitoefening van zijn FG taken, zoals deze blijken uit artikel 38 AVG.

6.2 Onderzoek

De FG kan een onderzoek instellen naar de wijze waarop in verband met de verwerking van persoonsgegevens, in een bepaald geval dan wel in het algemeen belang, de persoonlijke levenssfeer wordt beschermd.
De FG kan voor zijn onderzoek gebruik maken van de diensten van derden.
De FG deelt zijn bevindingen aan het betreffende bestuursorgaan mee en doet zo nodig aanbevelingen.

6.3 Register van verwerkingen

De FG houdt een register bij waarin verwerkingen van persoonsgegevens zijn vermeld. Het register vermeldt ten minste de volgende elementen:

- omschrijving van de verwerking;
- doel(en) van de verwerking;
- grondslag(en) van de verwerking;
- welke persoonsgegevens of categorieën van persoonsgegevens worden verwerkt;
- ontvangers of categorieën van ontvangers aan wie gegevens worden verstrekt;
- doorgifte van gegevens naar landen buiten de EU;
- de bewaartermijn.

7 Rechten van betrokkene

Als persoonsgegevens door de gemeente worden verwerkt, heeft degene van wie de persoonsgegevens worden verwerkt een aantal rechten. De teams of proceseigenaren voeren de taken uit met betrekking tot de rechten van betrokkene, zoals omschreven in de AVG. Het gaat hierbij om de volgende rechten:

- Recht op informatie: betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: betrokkenen hebben de mogelijkheid om te controleren of, en op welke wijze zijn of haar gegevens worden verwerkt.
- Correctierecht: als duidelijk wordt dat de gegevens niet juist zijn, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht van verzet: betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht op het wissen van persoonsgegevens: in gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene in een aantal in de AVG aangegeven gevallen, het recht om de persoonsgegevens te laten wissen.
- Recht op bezwaar: betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
- Recht op het doorgeven van informatie (dataportabiliteit): betrokkene heeft recht om gegevens beschikbaar gesteld te krijgen op een dergelijk manier dat betrokkene deze zelf gemakkelijk door kan geven aan een andere verwerkingsverantwoordelijke.

Indienen van een verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk, als via de website van de gemeente ingediend worden.

De gemeente verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De gemeente stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Als het verzoek niet wordt opgevolgd, is er de mogelijkheid om bezwaar te maken bij de gemeente. Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Als de gemeente een wettelijke verplichting niet nakomt, kan de betrokkene een klacht indienen. Op de website van de gemeente Berkelland maakt de gemeente bekend op welke manier dat mogelijk is.

Dit beleid treedt in werking na vaststelling door het college van burgemeester en wethouders. Het beleid wordt iedere drie jaar geëvalueerd en indien nodig herzien.

Aldus vastgesteld door burgemeester en wethouders van Berkelland
op 11 december 2018,

De gemeentesecretaris,
M. Broers

De burgemeester,
J.H.A. van Oostrum