gemeente HELLEVOETSLUIS

GEMEENTEBLAD

Officiële uitgave van de gemeente Hellevoetsluis

Nr. 152788

17 mei

2021

Privacybeleid gemeente Hellevoetsluis 2021

Nummer: 04-03-21/12

De raad der gemeente Hellevoetsluis;
Het college van burgemeester en wethouder der gemeente Hellevoetsluis, en;
De burgemeester der gemeente Hellevoetsluis

BESLUITEN

vast te stellen de Privacybeleidsregels gemeente Hellevoetsluis 2021.

Inhoudsopgave

1. Inleiding

Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor privacy op tactisch niveau en werkinstructies op operationeel niveau.

Binnen de gemeente Hellevoetsluis wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van persoonsgegevens en privacy. De gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Alle verantwoordelijke bestuursorganen van de gemeente, waaronder uiteraard de raad, het college van burgemeester en wethouders, burgemeester en het management spelen een cruciale rol bij het

waarborgen van privacy. De gemeente geeft middels dit beleid richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op alle in de gemeente Hellevoetsluis bestaande bestuursorganen alsmede op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacybeleid is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

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.

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 privacybeleid 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 privacybeleid hangt daarom ook nauw samen met het informatiebeveiligingsbeleid van de gemeente Hellevoetsluis, waarin de gemeente het geheel van technische- en organisatorische maatregelen beschrijft en daarmee ook invulling geeft aan de beveiliging van informatie en persoonsgegevens. Dit privacybeleid sluit tevens aan bij de I-visie van de gemeente Hellevoetsluis.

Dit beleid treedt in werking na vaststelling en daaropvolgend bekendmaking door de daartoe bevoegde bestuursorganen. Het beleid wordt periodiek geëvalueerd en indien nodig herzien.

Gelet op de voorgenomen bestuurlijke fusie tussen de gemeenten Brielle, Westvoorne en Hellevoetsluis, is ervoor gekozen om hoofdzakelijk hetzelfde privacybeleid te hanteren als van Brielle en Westvoorne. Hiermee wordt voldaan aan de afspraak dat beleid waar mogelijk in Voorns verband wordt opgesteld.

2. Visie en doelstelling bescherming van persoonsgegevens

Dit privacybeleid verwoordt de bestuurlijke visie van de bestuursorganen van de gemeente Hellevoetsluis op privacy zoals deze besloten ligt in de Europese en Nederlandse privacywetgeving.

2.1 Visie

De gemeente 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 privacybeleid, 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.

Privacybeleid is niet zozeer een extra last; het biedt ook voordelen. Door dit beleid is geborgd dat de privacy van medewerkers, burgers en andere betrokkene gewaarborgd zijn.

2.3 Reikwijdte

Dit privacybeleid 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 Baseline Informatiebeveiliging Overheid (de zogeheten BIO). 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

De burgemeester, het college van burgemeester en wethouders en de gemeenteraad zijn de verantwoordelijke voor verwerking van persoonsgegevens, zoals bedoeld in artikel 4 onder punt 7 van de AVG. Er zijn echter nog meer bestuursorganen binnen de gemeente, zoals de bezwaarcommissie en de heffingsambtenaar. Deze bestuursorganen stellen dit beleid niet rechtstreeks vast, maar voor hen zal gelden dat dit beleid als vaste gedragslijn dient te worden gehanteerd.

4.2 Verantwoordelijkheid voor uitvoering van beleid

De ambtelijke verantwoordelijkheid voor de uitvoering van beleid ligt voor zover het de burgemeester en het college van burgemeester en wethouders betreft bij de gemeentesecretaris. Daar waar het gaat om de raad is de griffier de ambtelijk verantwoordelijke. Aan deze verantwoordelijkheid wordt mede invulling gegeven door zorg te dragen voor voldoende kennis en bewustzijn van zorgvuldige verwerking van persoonsgegevens bij alle betrokken medewerkers.

4.3 Functionaris gegevensbescherming (FG)

De verantwoordelijke bestuursorganen benoemen 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 het management 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 Hellevoetsluis.

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;

- Sociale 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, dit wordt ook wel doelbinding genoemd. Bovendien bepaalt de wet dat persoonsgegevens slechts mogen worden verwerkt voor zover zij toereikend , ter zake dienend en niet bovenmatig zijn. Kortom, staat het doel van de verwerking in verhouding tot de inbreuk voor de personen van wie persoonsgegevens wordt verwerkt? Dit noemen we proportionaliteit.

Naast het begrip proportionaliteit kent de AVG het begrip subsidiariteit. Bij elke verwerking van persoonsgegevens moet worden bekeken of het doel ook op een andere wijze kan worden bereikt waarbij de inbreuk op de privacy van betrokkene minder is.

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 persoonsgegevensminstens één grondslag aanwezig moet zijn. De volgende grondslagen worden gehanteerd:

- Toestemming van betrokkene;
- Uitvoering van een overeenkomst;
- Noodzakelijk om te voldoen aan een wettelijke verplichting;
- Noodzakelijk om de vitale belangen te beschermen;
- Noodzakelijk voor de vervulling van een algemeen belang, of van een taak in kader van de uitoefening van het openbaar gezag;
- Noodzakelijk om gegevens te verwerken om een gerechtvaardigde belang te behartigen.

5.2 Uitgangspunten

Het wettelijk kader, zoals hiervoor beschreven, is bepalend bij het formuleren van de uitgangspunten van beleid. Het privacybeleid is gebaseerd 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 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 privacybeleid 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;
- 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 Data Privacy Impact assessment (DPIA)

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 middel van een DPIA. Door middel van een DPIA zal moeten worden aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd. Mocht er worden afgeweken van het advies van de te nemen maatregelen dan wordt dit gemotiveerd kenbaar gemaakt bij de FG.

Bij een ICT aanvraag wordt indien nodig een DPIA uitgevoerd.

Pas nadat de DPIA 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 DPIA uitgevoerd.

Over de inhoud van de DPIA wordt de FG 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. Het datalek dient uiterlijk binnen 72 uur te worden gemeld bij de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor 'de rechten en vrijheden van betrokkenen'. In dat geval zal geen melding van het datalek worden gemaakt bij de AP. De betrokken personen worden alleen geïnformeerd als er sprake is van een hoog risico voor de rechten en vrijheden van hen. De afhandeling van het datalek is de verantwoordelijkheid van de verwerkingsverantwoordelijke, die hierbij nauw contact onderhoudt met de FG. De FG houdt een bestand 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. Dit gebeurt bij een ICT aanvraagproces.

Onder privacy by design maatregelen verstaan wij onder meer het afsluiten van verwerkersovereenkomsten, toegangsbeveiliging, encryptie, het 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.

5.7 Register van verwerkingen

De verwerkingsverantwoordelijke 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

5.8 Beveiliging van de verwerking

De verwerkingsverantwoordelijke neemt passende technische en organisatorische maatregelen om te waarborgen dat er sprake is van een op de veiligheidsrisico's afgestemd niveau van beveiliging, waaronder ook de vertrouwelijkheid valt. De beveiligingsmaatregelen die zo nodig moeten worden genomen om een beveiligingsniveau te waarborgen dienen onder meer het volgende te omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

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 de gemeentesecretaris c.q. de griffier. 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 deelt zijn bevindingen aan het betreffende bestuursorgaan mee en doet zo nodig aanbevelingen.

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.

8. 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 (via DigiD) 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. Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Aldus besloten in de openbare vergadering van de raad, gehouden op 4 maart 2021.
Voor zover bevoegd de burgemeester voornoemd,
M.C. Junius

Voor zover bevoegd het college van burgemeester en wethouders voornoemd,
de secretaris,
S. Bronsveld
de burgemeester,
M.C. Junius

Voor zover bevoegd de raad voornoemd,
plaatsvervangend griffier,
M. Hoek
de voorzitter,
M.C. Junius