

Addendum Privacybeleid Wet Politiegegevens

Gemeente Hardinxveld-Giessendam
Vastgesteld door

College d.d.

Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente heeft in haar privacybeleid en informatiebeveiligingsbeleid vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens.

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen.

Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

Het huidige privacybeleid van de gemeente Hardinxveld-Giessendam gaat alleen uit van de AVG. Het is daarom wenselijk er de verplichtingen uit de Wpg aan toe te voegen.

Doelstellingen van het privacybeleid

Het privacybeleid van de gemeente beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit privacybeleid bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:

- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- De betrokkenen centraal stellen en het vertrouwen in een correcte omgang met hun gegevens vergroten;
- Gedrag vertonen dat past bij goed werknemerschap;
- De kans op financiële en imagoschade minimaliseren.

Wpg kader

Het normenkader van de Wpg is grotendeels gelijklopend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken met zowel AVG als Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk. De boa's binnen de gemeente Hardinxveld-Giessendam werken in de applicatie NatuurNetwerk BRS.

De hierna genoemde verplichtingen uit de Wpg zijn geborgd binnen onze applicaties:

- Er wordt een scheiding aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;

- Er wordt onderscheid gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van externe privacy audits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de Autoriteit Persoonsgegevens. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de Autoriteit Persoonsgegevens, uiterlijk 1 jaar na het uitvoeren van de externe audit.

Register van verwerkingen

Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

De Wpg processen zijn opgenomen in het verwerkingsregister iNavigator en voor het aanbrengen mutaties hierin bestaat een werkinstructie.

Informatiebeveiligingsbeleid

De gemeente Hardinxveld-Giessendam heeft een eigen informatiebeveiligingsbeleid. Dit is een richtinggevend en kaderstellend beleidsdocument. De gemeente vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten. Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

De informatiebeveiliging binnen de gemeente Hardinxveld-Giessendam vindt plaats volgens een algemeen erkende overheidsnorm (BIO).

De toereikendheid van de informatiebeveiliging blijkt uit de volgende certificering en verklaring van toepassingelijkheid:

- Eigen controles of eigen mededelingen over de beveiligingsmaatregelen
- Bevindingen gedaan en beschreven ten behoeve van ENSIA
- Strategisch beleid Informatiebeveiliging Drechtsteden 2025-2029
- Informatieveiligheidsplan Drechtsteden 2023

FG en bevoegd functionaris

De Functionaris Gegevensbescherming (FG)

Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

Rechten van betrokkenen

De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijklopend. De betrokkene heeft het recht:

- om uitsluitel te verkrijgen over of wij uw persoonsgegevens onder de Wpg van u gebruiken (artikel 24a WPG);
- om de persoonsgegevens die de gemeente onder de Wpg van u verwerkt in te zien (artikel 25 lid 1 WPG);
- onjuiste politiegegevens aan te laten passen naar juiste politiegegevens (artikel 28 lid 1 WPG);
- onvolledige politiegegevens aan te vullen, onder meer doormiddel van een aanvullende verklaring (artikel 28 lid 1 WPG);
- op vernietiging van politiegegevens (artikel 28 lid 2 WPG);
- op afscherming van politiegegevens (artikel 28 lid 2 WPG).

Het college van burgemeester en wethouders heeft het recht een verzoek af te wijzen als:

- het verzoek gerechtelijke onderzoeken of procedures zou belemmeren (artikel 27 lid 1 sub a WPG);
- dat nadelige gevolgen heeft voor het voorkomen van het begaan van strafbare feiten, voor opsporing, onderzoek, vervolging of het opleggen van straffen (artikel 27 lid 1 sub b WPG);
- de openbare veiligheid in het geding is (artikel 27 lid 1 sub c WPG);
- de rechten en vrijheden van derden worden geschonden (artikel 27 lid 1 sub d WPG);
- de nationale veiligheid in het geding is (artikel 27 lid 1 sub e WPG);
- de gemeente de wettelijke plicht heeft deze politiegegevens gegevens te bewaren (artikel 28 lid 2 sub b WPG);
- het kennelijk een ongegrond of buitensporig verzoek is (artikel 27 lid 1 sub f WPG).

In de privacyverklaring van de gemeente wordt toegelicht hoe deze rechten kunnen worden uitgeoefend.

Het bewaren van politiegegevens

Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar te worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Alle politiegegevens worden gelabeld in artikel 8, 9 en 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

Het ter beschikking stellen en verstrekken van politiegegevens

De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit 'need to know'-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.

Voor op de juiste manier gegevens ter beschikking stellen wordt gebruik gemaakt van de Verstrekkingwijzer van Suzanne Franken.
De applicatie BRS faciliteert in het vastleggen van de verstrekkingen.

Het melden van datalekken

De datalekprocedure onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijklopend. Op deze mededelingsplicht voor de Wpg zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Datalekken kunnen zowel intern als extern worden gemeld. Interne meldingen kunnen worden gedaan via het daarvoor ontworpen formulier dat op het intranet van de gemeente Hardinxveld-Giessendam staat. Dit formulier geeft de mogelijkheid tot het melden van datalekken die specifiek zien op politiegegevens.

Externe meldingen, bijvoorbeeld door inwoners, kunnen zowel telefonisch als via e-mail worden gemeld. Meer informatie hierover is te vinden op de gemeentelijke website. Voor de afhandeling van zowel interne als externe meldingen is er een procedure. De privacy coördinator van de gemeente draagt zorg voor de afhandeling van de melding. De functionaris gegevensbescherming wordt over alle meldingen geïnformeerd en adviseert indien nodig.

Bewustwording

Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Elke nieuwe medewerker moet daarom verplicht een Wpg training doorlopen.

Bij gebruik van de applicatie BRS geldt daarnaast dat pas nadat leverancier NatuurNetwerk het succesvol afronden van de cursus voor gebruik van BRS heeft gecontroleerd verleent zij de nieuwe medewerker toegang tot BRS.

Daarvan wordt een notitie vastgelegd in het personeelsdossier. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek Wpg-onderwerp of in de vorm van een toets. Ook van deelname aan deze initiatieven wordt een notitie in het personeelsdossier gemaakt.

Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring die op de website is te vinden.