

Privacybeleid gemeente Waterland 2023

Het college van burgemeester en wethouders van Waterland,

gelet op het gestelde in de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Wet politiegegevens (Wpg)¹, Besluit politiegegevens (Bpg), Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens;

overwegende dat het wenselijk is het "Privacybeleid gemeente Waterland 2019" in te trekken en regels vast te stellen hoe om te gaan met de verwerking en bescherming van zowel persoonsgegevens als politiegegevens binnen de gemeente Waterland,

BESLUIT:

vast te stellen het navolgende Privacybeleid gemeente Waterland 2023.

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1. Definities en begripsbepaling

In dit besluit wordt verstaan onder:

- a. Autoriteit Persoonsgegevens (AP): de landelijke toezichthouder die toeziet of persoonsgegevens op een juiste manier worden verwerkt;
- b. betrokkene: de persoon op wie de persoonsgegevens betrekking hebben, degene van wie de gegevens worden verwerkt;
- c. buitengewoon opsporingsambtenaar (boa): de boa's van de gemeente kunnen naast hun opsporingsstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. De verwerking van persoonsgegevens door de boa's valt zowel onder de AVG als de Wpg;
- d. datalekken: van datalekken is sprake wanneer persoonsgegevens verloren gaan of in handen vallen van onbevoegden, die geen toegang tot die gegevens mogen hebben;
- e. Functionaris Gegevensbescherming (FG): intern toezichthouder op de verwerking en bescherming van persoonsgegevens;
- f. gegevensbeschermingseffectbeoordeling: in een vroeg stadium op een gestructureerde en heldere manier de effecten en privacy risico's van nieuwe en bestaande verwerkingen in beeld brengen en welke maatregelen getroffen dienen te worden aan de hand van de geconstateerde risico's. Dit wordt ook wel een (Data) Privacy Impact Assessment (PIA of DPIA) genoemd;
- g. gemeente: de gemeente Waterland;
- h. persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Of wel, alle gegevens waaraan je een mens direct of indirect als individu kunt herkennen. Elk gegeven dat te herleiden is tot een bepaald persoon. Gegevens zoals naam, adres, woonplaats en bijzondere gegevens, zoals etnische achtergrond, politieke voorkeuren, gezondheid of het Burgerservicenummer (BSN);
- i. politiegegevens: persoonsgegevens die in het kader van een politietaak worden verwerkt;
- j. profilering: hiervan is sprake wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt, waarbij aan de hand van die gegevens naar bepaalde persoonlijke aspecten wordt gekeken om deze persoon te categoriseren, te analyseren of om zaken te kunnen voorspellen;
- k. verwerker: de persoon of organisatie die de persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke verwerkt en zelf geen zeggenschap heeft over het doel en de middelen van de verwerking;
- l. verwerking: alles wat met een persoonsgegeven wordt gedaan, zoals verzamelen, vastleggen, bewaren, samenvoegen, verspreiden, delen, opvragen, lezen, wijzigen en uitwissen of vernietigen;
- m. verwerkingsverantwoordelijke: de bestuursorganen van de gemeente Waterland die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

1) Voor dit Privacybeleid is ten aanzien van de Wet politiegegevens en aanverwante regelingen die van toepassing zijn op de verwerking van politiegegevens gebruik gemaakt van het "Addendum privacybeleid Wet politiegegevens" en het "Addendum Rechten van betrokkenen Wet politiegegevens" van de Vereniging van Nederlandse Gemeenten/Informatiebeveiligingsdienst voor gemeenten, licentie onder: CC BY-NC-SA 4.0.

Artikel 2. Doel

Dit beleid beschrijft hoe de gemeente verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaat. De verwerkingsverantwoordelijke is verplicht om behoorlijk, zorgvuldig en veilig om te gaan met de verwerking van persoonsgegevens. Daarnaast heeft de verwerkingsverantwoordelijke een verplichting om transparant te zijn en een informatieplicht richting de betrokkenen. Dit beleid is erop gericht de privacy van inwoners, medewerkers en (keten)partners te waarborgen en persoonsgegevens te beschermen tegen onrechtmatige verwerking. De gemeente wil met dit beleid onder andere bereiken dat medewerkers, waaronder de boa's, zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met persoons- en politiegegevens en het vertrouwen van betrokkenen in de overheid niet beschamen.

Artikel 3. Reikwijdte

Dit beleid is van toepassing op de gemeentelijke organisatie van de gemeente Waterland en heeft betrekking op de persoonsgegevens van personen van wie de verwerkingsverantwoordelijke gegevens verwerkt of laat verwerken.

Artikel 4. Wettelijke kaders

De verwerkingsverantwoordelijke is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het Privacybeleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- a. Algemene verordening Gegevensbescherming (AVG);
- b. Uitvoeringswet Algemene Verordening Gegevensbescherming;
- c. Wet Basisregistratie Personen;
- d. Wet politiegegevens (Wpg);
- e. Besluit politiegegevens (Bpg);
- f. Besluit politiegegevens buitengewoon opsporingsambtenaren;
- g. Regeling periodieke audit politiegegevens.

HOOFDSTUK 2. VERWERKING VAN PERSOONSgegevens

Artikel 5. Uitgangspunten voor de verwerking van persoonsgegevens

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

1. Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
2. Voor de verwerking van persoonsgegevens moet een rechtmatige grondslag zijn. Persoonsgegevens worden alleen verwerkt als aan tenminste één van de wettelijke grondslagen wordt voldaan:
 - a. om een verplichting na te komen die in de wet staat;
 - b. voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
 - c. om vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen, bijvoorbeeld een ernstige bedreiging van de gezondheid;
 - d. voor de goede vervulling van de gemeentelijke taak;
 - e. voor de behartiging van een gerechtvaardigd belang;
 - f. wanneer de betrokkene vrij en expliciet toestemming heeft gegeven voor een specifieke verwerking.
3. Alleen in uitzonderlijke gevallen wordt vooraf om toestemming gevraagd. Betrokkenen zijn veelal afhankelijk van de gemeente. Er is dan geen sprake van vrije toestemming. Voor een rechtmatige verwerking moet dan aan tenminste één van de andere voorwaarden als bedoeld in het tweede lid worden voldaan.
4. Persoonsgegevens worden alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en verwerkt. Het doel voor de verwerking moet duidelijk zijn en van tevoren zijn bepaald.
5. Persoonsgegevens worden alleen verwerkt als dat noodzakelijk is voor het vooraf bepaalde doel. De verwerkingsverantwoordelijke streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
6. Persoonsgegevens worden niet verwerkt als er een manier voorhanden is die minder inbreuk maakt op de privacy van betrokkenen. De inbreuk op de belangen van betrokkenen mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.
7. De verwerkingsverantwoordelijke gaat zorgvuldig met persoonsgegevens om en behandelt deze vertrouwelijk. De kwaliteit van de gegevens wordt gewaarborgd en persoonsgegevens worden alleen verwerkt door bevoegde personen met een geheimhoudingsplicht. Daarbij zorgt de verwer-

- kingsverantwoordelijke voor passende beveiliging van de persoonsgegevens conform het vastgestelde informatiebeveiligingsbeleid.
8. In het kader van zorgvuldige omgang met persoonsgegevens volgt elke nieuwe medewerker verplicht een training bewustzijn inzake informatiebeveiliging. Nieuwe boa's volgen daarnaast een Wpg-training. Periodiek, zo mogelijk jaarlijks, is er aanvullend aandacht voor bewustwording.
 9. Bij samenwerking met externe partijen waarbij sprake is van verwerking van persoonsgegevens, of als de verwerkingsverantwoordelijke persoonsgegevens laat verwerken door een verwerker, maakt de verwerkingsverantwoordelijke afspraken over de eisen waaraan de verwerking en/of gegevensuitwisseling moet voldoen. Deze afspraken worden vastgelegd in een (verwerkers)overeenkomst die voldoen aan de wet- en regelgeving.
De verwerkingsverantwoordelijke controleert of de gemaakte afspraken worden nageleefd.
 10. Persoonsgegevens worden zo veel mogelijk bij de betrokkene zelf verzameld.
 11. De verwerkingsverantwoordelijke informeert betrokkenen over het verwerken van persoonsgegevens.
 12. Bij verzoeken om informatie bekijkt de verwerkingsverantwoordelijke of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van de betrokkene. In principe worden geen persoonsgegevens verstrekt, tenzij dat (wettelijk) verplicht is.
 13. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. Het bewaren van persoonsgegevens kan nodig zijn om gemeentelijke taken goed uit te voeren of een wettelijke verplichting te kunnen naleven. Zo kent de Wpg bijvoorbeeld, in tegenstelling tot de AVG, specifieke bewaartermijnen voor de opslag van politiegegevens.

Artikel 6. Aanvullende uitgangspunten Wpg

1. In de verwerking van gegevens door boa's is een onderscheid gemaakt welke gegevens worden verwerkt onder de AVG en welke onder de Wpg.
2. Gegevens die op feiten zijn gebaseerd worden gescheiden van gegevens die op een persoonlijk oordeel zijn gebaseerd.
3. Onderscheid wordt gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden.
4. De Wpg stelt andere eisen bij het delen van politiegegevens tussen verschillende partijen.
 - a. Politiegegevens worden gedeeld met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk (ter beschikking stellen binnen het Wpg-domein). Hierbij wordt een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging gemaakt.
 - b. Bij het verstrekken van politiegegevens buiten het Wpg-domein wordt geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein voor zover dat noodzakelijk is voor de doeleinden als in de Wpg en Bpg benoemd, vereist is bij wet en in overeenstemming met het bevoegd gezag.
5. Doelen van onderzoeken, verstrekking of doorgifte (buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens), afwijzing van verzoeken om inzage en inbreuken op de beveiliging worden gedocumenteerd.
6. Er vindt logging plaats in de geautomatiseerde systemen op invoer van gegevens en (op termijn) van het verzamelen, wijzigen, raadplegen, verstrekken, combineren of vernietigen van politiegegevens.
7. Politiegegevens worden gecategoriseerd en niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door toepasselijke wet- en regelgeving, of voor het doeleinde waarvoor ze zijn verwerkt. Politiegegevens worden na verwijdering (afgeschermd en niet meer in te zien) nog maximaal vijf jaar bewaard. Daarna of daarbinnen, afhankelijk van de geldende bewaartermijn, vindt definitieve vernietiging plaats en zijn de gegevens niet meer terug te halen.
8. Voor de definitieve vernietiging mogen verwijderde, afgeschermd politiegegevens, opnieuw worden verwerkt en dus ook geraadpleegd als:
 - a. de Officier van Justitie hiertoe namens de politie opdracht voor geeft als er een groot opsporingsonderzoek moet worden verricht, dat een grote impact op de rechtsorde kan hebben.
 - b. de verwerkingsverantwoordelijke de gegevens nodig heeft ter verantwoording of voor bijvoorbeeld een klachtenprocedure.
9. Ingeval van cultureel of historisch belang kan worden afgezien van vernietiging en wordt aan de bewaareisen genoemd in de Archiefwet voldaan.
10. Gemeenschappelijke verwerkingen worden gemeld bij de AP.
11. Het verwerken van politiegegevens wordt conform de wetgeving in- en extern ge-audit. De rapportage van de externe audit wordt verstrekt aan de AP.

Artikel 7. Geautomatiseerde verwerkingen

1. De verwerkingsverantwoordelijke maakt geen gebruik van profilering waarbij aan de hand van persoonsgegevens naar bepaalde aspecten van een persoon wordt gekeken om deze persoon te categoriseren, te analyseren, zaken te voorspellen of om geautomatiseerde besluiten te nemen.
2. De verwerkingsverantwoordelijke maakt geen gebruik van Big data en tracking. Als dat in de toekomst wel het geval is, dan mogen de gegevens in Big data en tracking alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon. En mogen ze alleen worden verzameld voor onderzoek dat door of namens de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Onder bepaalde omstandigheden kan de verwerkingsverantwoordelijke voor het vergroten van de veiligheid op straat gebruik maken van cameratoezicht.

HOOFDSTUK 3. PLICHTEN VAN DE VERWERKINGSVERANTWOORDELIJKE

Artikel 8. Informatieplicht

1. Wanneer verwerking van persoonsgegevens plaatsvindt moet het voor de betrokkenen duidelijk zijn dat dit zo is en wat het doel is van de verwerking.
2. De verwerkingsverantwoordelijke informeert de betrokkenen actief voorafgaand aan de verwerking en op een heldere en toegankelijke manier.
3. Wanneer betrokkenen gegevens aan de verwerkingsverantwoordelijke verstrekken, bijvoorbeeld via een formulier, worden zij geïnformeerd over de manier waarop de verwerkingsverantwoordelijke met de persoonsgegevens omgaat.
4. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de verwerkingsverantwoordelijke persoonsgegevens van hem/haar verzamelt en verwerkt en weet waarom en voor welk doel dat gebeurt.

Artikel 9. Register van verwerkingen

1. De verwerkingsverantwoordelijke houdt een register bij van alle verwerkingen van persoonsgegevens waarvoor de verwerkingsverantwoordelijke verantwoordelijk is.
2. In het register zijn een aantal gegevens opgenomen, waaronder:
 - a. de naam en contactgegevens van de verwerkingsverantwoordelijke en, als dat het geval is, de gezamenlijke verwerkingsverantwoordelijke en van de functionaris gegevensbescherming;
 - b. de naam en contactgegevens van de eventuele verwerker;
 - c. het doel of de doelen van de verwerking;
 - d. de rechtmatigheid en grondslag van de verwerking, met inbegrip van doorgiften;
 - e. een beschrijving van het soort persoonsgegevens en daarbij behorende categorieën van betrokkenen;
 - f. een beschrijving van de ontvangers van de persoonsgegevens;
 - g. een beschrijving van het delen/verstrekken van persoonsgegevens;
 - h. de bewaartermijn van de gegevens, zo mogelijk de beoogde termijn waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;
 - i. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen;
 - j. (Wpg) in voorkomend geval: het gebruik van profilering;
 - k. (Wpg) in voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of internationale organisatie;
 - l. (Wpg) de toekenning van de autorisaties.

Artikel 10. Gegevensbeschermingseffectbeoordeling/Privacy Impact Assessment

1. Op het moment dat er sprake is van een verhoogd risico bij het gebruik van de persoonsgegevens, brengt de verwerkingsverantwoordelijke de effecten en privacy risico's in kaart door een Privacy Impact Assessment (PIA). Op basis van de PIA neemt de verwerkingsverantwoordelijke maatregelen om de privacy risico's zo veel mogelijk weg te nemen.
2. Voor nieuwe verwerkingen is het uitvoeren van een PIA verplicht.
3. Pas nadat een PIA is uitgevoerd en de maatregelen zijn getroffen die nodig zijn om de risico's te beperken, verwerkt de verwerkingsverantwoordelijke de persoonsgegevens.

Artikel 11. Functionaris Gegevensbescherming

1. De verwerkingsverantwoordelijke heeft een Functionaris Gegevensbescherming (FG) aangesteld als intern toezichthouder voor zowel de AVG als de Wpg.
2. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoons- en politiegegevens.
3. De taken van de FG zijn informeren, adviseren, toezicht houden, bewustwording creëren en optreden als contactpersoon van de Autoriteit Persoonsgegevens.

4. De taken op het gebied van de bescherming van de privacy is de eigen verantwoordelijkheid van de proceseigenaar/vak-afdeling van de organisatie.
5. De FG is het aanspreekpunt voor betrokkenen en moet goed bereikbaar zijn binnen en buiten de organisatie. De contactgegevens van de FG zijn vermeld op de website van de gemeente.

Artikel 12. Bevoegd functionaris Wpg

1. Het aanwijzen van een bevoegd functionaris Wpg (BF) conform artikel 2:10, eerste lid Bpg is verplicht ten aanzien van de politiegegevens die onder artikel 9 Wpg (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval) worden verwerkt. De gemeente Waterland verwerkt uitsluitend persoonsgegevens die vallen onder artikel 8 Wpg (verwerking in het kader van de politietaak). Omdat daarvoor geen BF nodig is, heeft de gemeente geen BF aangesteld.

Artikel 13. Datalekken

1. De gemeente heeft een proces ingericht voor het melden van mogelijke beveiligingsincidenten en/of datalekken, zowel voor meldingen vanuit de organisatie als daarbuiten.
2. Voor het melden van (mogelijke) datalekken is een centraal meldpunt beschikbaar (meldpunt datalekken).
3. Op de website van de gemeente is op de pagina informatieveiligheid/privacy een online formulier beschikbaar voor het melden van (mogelijke) datalekken bij het centrale meldpunt als bedoeld in het tweede lid.
4. Wanneer een datalek heeft plaatsgevonden wordt direct actie ondernomen om de schade te beperken en (verdere) nadelige gevolgen te voorkomen.
5. Datalekken worden door de verwerkingsverantwoordelijke zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de Autoriteit Persoonsgegevens. Als dit later is dan 72 uur wordt daarvoor een motivering bij de melding gevoegd.
6. Als de inbreuk een hoog risico meebrengt voor de rechten en vrijheden van betrokkenen, wordt de inbreuk in eenvoudige en duidelijke taal aan de betrokkenen gemeld.
7. Datalekken worden gedocumenteerd en de verwerkingsverantwoordelijke houdt een register bij van meldingen van beveiligingsincidenten en datalekken.
8. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.
9. Specifiek voor de Wpg zijn op de meldingsplicht enkele uitzonderingen van toepassing. Bijvoorbeeld als de melding achterwege moet blijven ter vermijding van belemmering van gerechtelijke onderzoeken of procedures, ter vermijding van nadelige gevolgen voor voorkoming, opsporing, onderzoek en vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

HOOFDSTUK 4. RECHTEN VAN BETROKKENEN

Artikel 14. Rechten van betrokkenen

1. Betrokkenen van wie de verwerkingsverantwoordelijke persoonsgegevens verwerkt, hebben het recht om na te gaan wat er met hun gegevens gebeurt en als dat nodig is hier invloed op uit te oefenen. Deze rechten zijn:
 - a. recht op informatie: betrokkenen hebben het recht om aan de verwerkingsverantwoordelijke te vragen of zijn of haar gegevens door de verwerkingsverantwoordelijke worden verwerkt;
 - b. recht op inzage: betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn of haar eigen gegevens worden verwerkt. Om welke gegevens het gaat, wie de gegevens heeft ingezien en aan wie de gegevens worden verstrekt;
 - c. correctierecht: als duidelijk wordt dat de gegevens niet juist zijn, kan de betrokkene bij de verwerkingsverantwoordelijke een verzoek indienen om dit te corrigeren of aan te vullen;
 - d. recht om vergeten te worden: het recht om gegevens te laten verwijderen/vernietigen, tenzij legitieme wettelijke eisen dit voorkomen. In gevallen dat de betrokkene toestemming heeft gegeven voor de verwerking, heeft de betrokkene het recht om die toestemming net zo eenvoudig in te trekken en de gegevens te laten verwijderen/wissen;
 - e. recht van verzet: betrokkenen hebben het recht om aan de verwerkingsverantwoordelijke te vragen om hun persoonsgegevens niet meer te gebruiken. De verwerking moet dan worden gestaakt, tenzij er gerechtvaardigde gronden zijn voor de verwerking;
 - f. recht op bezwaar: betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn of haar persoonsgegevens en deze tijdelijk "stil" te laten zetten. De verwerkingsverantwoordelijke zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking;
 - g. recht op het doorgeven van informatie (dataportabiliteit): betrokkene heeft het recht om gegevens beschikbaar gesteld te krijgen op een dergelijke manier dat betrokkene deze zelf gemakkelijk door kan geven aan een andere verwerkingsverantwoordelijke;
 - h. recht om niet onderworpen te worden aan geautomatiseerde besluitvorming, waaronder profilering.

Artikel 15. Verzoeken in het kader van uitoefening van de rechten van betrokkenen

1. Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit kan zowel schriftelijk per post als via de e-mail als via de website van de gemeente ingediend worden.
2. De betrokkene kan alleen een verzoek indienen of gegevens opvragen over zichzelf en als de indiener ouder is dan 16 jaar en niet onder curatele is gesteld. Voor minderjarigen jonger dan 12 jaar wordt een inzageverzoek door de ouder(s) of wettelijke vertegenwoordiger gedaan. Voor jongeren van 12 tot 16 jaar dienen de ouder(s) of wettelijke vertegenwoordiger samen en met instemming van de jongere het verzoek in. Voor een onder curatele gestelde dient de curator het verzoek in.
3. Verzoeken conform de Wpg kunnen daarnaast worden ingediend door een advocaat aan wie de betrokkene een bijzondere machtiging heeft verleend met het oog op de uitoefening van zijn rechten krachtens deze wet en die het verzoek uitsluitend doet in het belang van zijn cliënt.
4. Verzoeken worden in behandeling genomen en gecoördineerd door de Privacy Officer (PO). De PO stemt de inhoudelijke behandeling van het verzoek af met de primaat houdende afdeling (lijnmanager/proceseigenaar), Juridische Zaken en/of senior boa.
5. De verwerkingsverantwoordelijke respecteert en honoreert de rechten van betrokkenen, tenzij legitieme wettelijke eisen die op de verwerkingsverantwoordelijke rusten dit voorkomen.
6. Het verstrekken van de informatie of het treffen van maatregelen geschiedt kosteloos, tenzij verzoeken van een betrokkene aantoonbaar ongegrond of buitensporig zijn. In dat geval wordt een redelijke vergoeding aangerekend of geweigerd gevolg te geven aan het verzoek.
7. De verwerkingsverantwoordelijke 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. Een gehele of gedeeltelijke afwijzing van een verzoek is schriftelijk en bevat de redenen voor de afwijzing.
8. Afhankelijk van de complexiteit van het verzoek kan de termijn indien nodig met maximaal twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
9. De Wpg schrijft voor dat de verwerkingsverantwoordelijke de beslissing maximaal vier weken kan verdagen, dan wel ten hoogste zes weken als blijkt dat verschillende regionale eenheden of bij de landelijke eenheid van politie politiegegevens over de verzoeker worden verwerkt. Van deze verdaging wordt schriftelijk mededeling gedaan.
10. Aan de hand van het verzoek kan de verwerkingsverantwoordelijke aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene en er voor te zorgen dat het verzoek duidelijk is.
11. De identiteit moet in persoon met geldige legitimatie worden vastgesteld, bijvoorbeeld middels gebruik van DigiD of aan de balie van het Klanten Contact Centrum van het gemeentehuis. Als de identiteit niet met voldoende zekerheid kan worden vastgesteld, is dit grond om het verzoek af te wijzen.
12. Bij een inzageverzoek op basis van de Wpg wordt informatie opgeleverd inzake doel en grondslag van de verwerking, de betrokken categorieën van politiegegevens, categorieën van ontvangers, de voorziene periode van opslag of criteria voor het bepalen van de termijn en de herkomst van de verwerking. Bij het inzageverzoek worden geen documenten verstrekt, maar wordt de betrokkene in de gelegenheid gesteld op locatie op inzage te komen. Hierbij mogen geen foto's en/of kopieën worden gemaakt.
13. Betrokkene heeft de mogelijkheid om bezwaar te maken bij de verwerkingsverantwoordelijke tegen een besluit op het verzoek als bedoeld in lid 1.
14. Betrokkene heeft de mogelijkheid om bij een vermoeden dat de verwerkingsverantwoordelijke zich niet aan de Privacywet houdt een klacht in te dienen bij de AP.

Artikel 16. Aanvullende beperkingen Wpg

1. Een verzoek om inzage, rectificatie en/of aanvulling en/of vernietiging van politiegegevens wordt afgewezen als dat noodzakelijk en evenredig is:
 - a. ter vermijding van belemmering van gerechtelijke onderzoeken of procedures;
 - b. ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
 - c. ter bescherming van de openbare veiligheid;
 - d. ter bescherming van de rechten en vrijheden van derden;
 - e. ter bescherming van de nationale veiligheid;
 - f. ingeval van een kennelijk ongegrond of buitensporig verzoek.
2. Een gehele of gedeeltelijke afwijzing van een verzoek is schriftelijk en bevat de redenen voor de afwijzing.

HOOFDSTUK 5. Evaluatie, beschikbaarheid en inwerkingtreding

Artikel 17. Evaluatie en beschikbaarheid

Het Privacybeleid wordt iedere drie jaar geëvalueerd en indien nodig herzien. Het beleid is te vinden op het intranet en de website van de gemeente Waterland en wordt gepubliceerd op Mijnoverheid.nl.

Artikel 18. Intrekking oude regeling

Het Privacybeleid gemeente Waterland 2019 wordt ingetrokken.

Artikel 19. Inwerkingtreding

Dit Privacybeleid treedt in werking de dag na bekendmaking.

Artikel 20. Citeertitel

Dit beleid wordt aangehaald als: Privacybeleid gemeente Waterland 2023.

Aldus besloten in de vergadering van het college van burgemeester en wethouders van de gemeente Waterland, gehouden op 07-12-2023

College van burgemeester en wethouders gemeente Waterland,

*drs. E.G.H. Dijk MPM
gemeentesecretaris/algemeen directeur*

*drs. M.C. van der Weele
burgemeester*