gemeente BERGEN Limburg

GEMEENTEBLAD

Officiële uitgave van de gemeente Bergen (L)

Nr. 470717

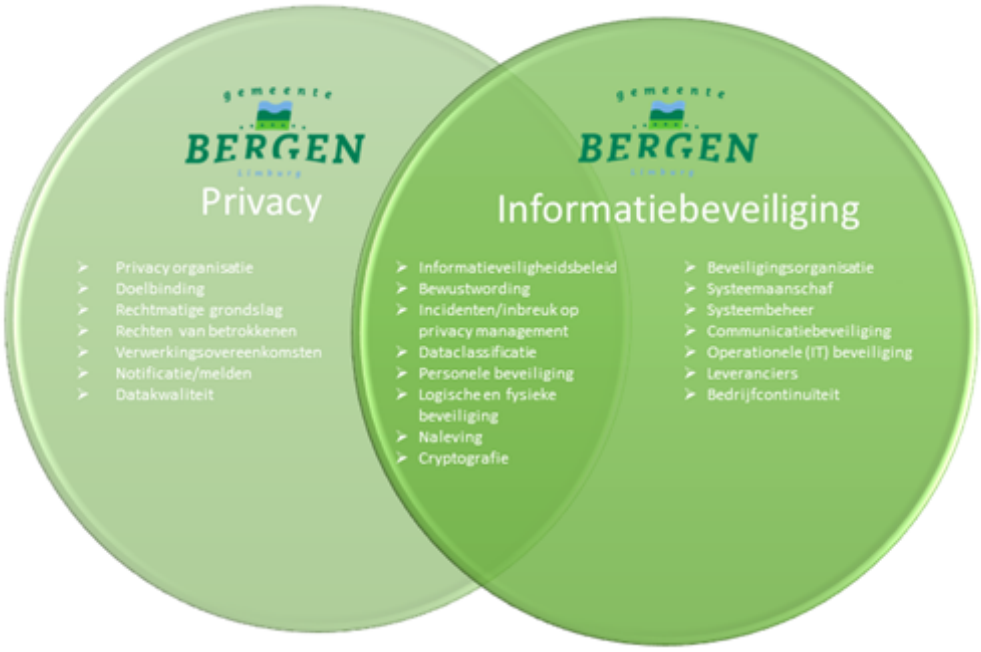
8 november 2024

Beleid Wet politiegegevens 2023-2026

Inleiding

De gemeente Bergen (L) heeft in haar privacybeleid[1] vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). Als ook het garanderen dat behoorlijk en zorgvuldig wordt omgegaan met (persoons)gegevens, om de persoonlijke levenssfeer, ofwel de privacy, van betrokkenen te beschermen. Een goede omgang met (persoons)gegevens zorgt voor betrouwbaarheid, en ook voor een goede kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen. De Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) zijn het wettelijk kader voor het privacybeleid.

Er is een nauwe samenhang tussen privacy en informatiebeveiliging. Het zijn twee verschillende begrippen maar hebben wel een gemeenschappelijk raakvlak. Privacy gaat over het vertrouwelijk omgaan met persoonlijke gegevens en deze dus ook voldoende beschermen. Informatieveiligheid gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie. Het privacybeleid kan door deze samenhang niet los worden gezien van het informatiebeveiligingsbeleid.



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. Dit beleidsstuk is een aanvulling op het Strategisch informatiebeveiligings- en privacybeleid en geeft invulling aan de verplichtingen uit deze wetten en regelgevingen.

Op enkele gebieden verschilt de Wpg ten opzichte van de AVG. 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

1) Dit Privacybeleid is te vinden op: https://lokaleregelgeving.overheid.nl/CVDR684079/1

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.

Dit beleidsstuk is dient als een aanvulling (addendum) op het bestaande privacybeleid van de gemeente beschouwd te worden voor het specifieke onderdeel van de Wpg.

Visie
Inwoners van de gemeente Bergen kunnen erop vertrouwen dat de gemeente hun privacy respecteert en zorgvuldig omgaat met hun persoonsgegevens. Privacybescherming is een onderwerp dat voor bestuurders en medewerkers een integraal onderdeel van het werk vormt.

Doelstellingen
Dit beleidsstuk strekt ertoe te beschrijven hoe er in de gemeente Bergen binnen wettelijke kaders verantwoordelijk op een verantwoorde wijze met persoonsgegevens omgaan. De gemeente wil met dit addendum 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;
- Het vertrouwen van betrokkenen in de overheid niet beschamen;
- Gedrag vertonen dat past bij goed werknemerschap;
- De kans op financiële en imagoschade minimaliseren.

Reikwijdte en doelbinding
Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente Bergen en haar opdrachtnemers voor zover deze persoonsgegevens verwerken en deze persoonsgegeven verwerkt worden in het kader van de uitvoering van de politietaken door Boa’s en hen eventueel daarbij behulpzame personen of geautomatiseerde systemen die geen Boa’s zijn.

Voor de omgang met persoonsgegevens gelden onder andere de volgende wettelijke kaders:

- De Europese Verordening;
- De Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
- Artikel 8 Europees Verdrag voor de Rechten van de mens en de fundamentele vrijheden;
- Artikelen 10 en 13 Grondwet (persoonlijke levenssfeer en briefgeheim);
- Sectorale wetgeving;
- Archiefwet;
- Wet politiegegevens (Wpg);
- Besluit politiegegevens (Bpg);
- Besluit politiegegevens buitengewoon opsporingsambtenaren;
- Interne kaders;
- Informatiebeveiligingsbeleid;
- Integriteitsbeleid;

Dit beleid wordt ondersteund door verschillende procedures en documentatie die in meer detail beschrijven hoe de principes die in dit beleid worden vermeld, zijn geïmplementeerd en uitgevoerd.

Het beleid met betrekking tot de Wet politiegegevens (Wpg) heeft betrekking op de manier waarop een gemeente Bergen omgaat met persoonsgegevens welke beschouwd worden als politiegegevens.

In de gemeentelijke organisatie worden politiegegevens verwerkt in het kader van de strafrechtelijke handhaving van overtredingen met betrekking tot de regels van de openbare ruimte waartegen de BOA’s van de Domeinen I (Openbare Ruimte) en II (Milieu, welzijn en infrastructuur) op kunnen treden.

Het gaat in de gemeente Bergen dus om de verwerking van politiegegevens door of namens de blauwe (Domein I) en groene BOA’s (Domein II). In het kader van de Leerplichtwet worden geen Wpg-gegevens verwerkt in de gemeente Bergen.

Bij de gemeente Bergen zijn meerdere BOA’s van de Domeinen I en II in dienst. Zij zijn belast met handhavingstaken en verwerken in dat kader persoonsgegevens. Als zij tijdens hun werkzaamheden strafbare feiten constateren, verwerken zij persoonsgegevens in het kader van de opsporingstaak. Op die verwerking is dan de Wpg van toepassing, wat inhoudt dat de verwerking van persoonsgegevens

plaatsvindt in het kader van de uitvoering van de (ondersteuning van) de politietaak als bedoeld in artikel 3 Politiewet. Net als de AVG stelt de Wpg eisen aan de verwerking van persoonsgegevens.

Gemeente Bergen verwerkt geen politiegegevens als bedoeld in de artikelen 9, 11 en 13 Wpg
Artikel 9 Wpg maakt het mogelijk om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van een milieudelict. Ook een gericht onderzoek naar het vergiftigen dieren of dumping van asbest kan onder dit artikel vallen, bijvoorbeeld als je verwacht dat het onderzoek langer dan veertig uur duurt of als er meerdere opsporingsambtenaren bij betrokken zijn. Artikel 9-gegevens mogen worden verwerkt tot het doel bereikt is.

In artikel 11 Wpg is het mogelijk gemaakt om gegevens te verwerken die geautomatiseerd vergeleken kunnen worden en in combinatie met andere gegevens geanalyseerd kunnen worden. Voor zover het voor een onderzoek noodzakelijk is kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens worden vergeleken om verbanden aan te tonen. De gerelateerde gegevens kunnen, na instemming van een daartoe bevoegde functionaris, voor dat onderzoek verder worden verwerkt.

Artikel 13 biedt tenslotte de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van de Wet politiegegevens verder te verwerken. De verwerkingsverantwoordelijke kan zelf een artikel 13-verwerking starten.

In de gemeentelijke organisatie van Bergen worden geen politiegegevens als bedoeld in de artikelen 9, 11 en 13 Wpg verwerkt.

Uitgangspunten (Wpg)
De in het gemeentelijke privacybeleid en privacyreglement neergelegde uitgangspunten van de AVG (normenkaders) zijn grotendeels gelijk aan die van de Wpg. Op hoofdlijnen geldt aanvullend voor de Wpg nog het volgende:

- De boa's van handhaving (domein I) en milieu, welzijn en infrastructuur (domein II) van de gemeente Bergen kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de 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 Wpg kent een aantal verplichtingen, die veelal geborgd binnen onze applicaties:

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er moet onderscheid worden 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 een externe privacy audits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een her-controle plaatsvindt. De her-controle geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de her-controle worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

Register van verwerkingen
De gemeente houdt een register van hun verwerkingsactiviteiten voor zowel de AVG als de Wpg bij waarin een overzicht wordt gegeven van de verschillende processen die bij de gemeente worden uit-

gevoerd en welke soorten persoonsgegevens worden verwerkt. Iedere afdeling heeft de verplichting dit register van verwerkingen op to date te houden. De privacy officer gecontroleerd periodiek dit register om de juistheid en volledigheid te waarborgen.

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. (*)

Rechten van betrokkenen

De rechten van betrokkenen onder de AVG staan beschreven in het bestaande privacybeleid en de privacyverklaring van de gemeente Bergen. Dat beleid voorziet ook in de verplichtingen die voortvloeien uit de Wpg. Binnen dit beleid worden de volgende rechten van betrokkenen geborgd:

- Recht op informatie: Betrokkenen worden door de gemeente geïnformeerd op het moment dat zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om in te zien of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht om vergeten te worden: Betrokken hebben het recht om persoonsgegevens te laten verwijderen, bijvoorbeeld indien de betrokkene zijn toestemming intrekt of de gegevens niet langer nodig zijn. De gemeente stelt eventuele partners van de gemeente, als deze de gegevens ook hebben, op de hoogte dat de betrokkene ook bij hen ‘vergeten’ moet worden.
- Recht op beperking: De betrokkene heeft het recht om een verzoek in te dienen tot beperking van de gegevensverwerking, bijvoorbeeld wanneer de betrokkene de juistheid van de gegevens betwist.
- Recht op overdraagbaarheid: Betrokkene heeft het recht op overdraagbaarheid van zijn/haar persoonsgegevens, ofwel dataportabiliteit. Dit houdt in dat betrokkene zijn gegevens op zo’n manier ontvangt dat hij/zij deze weer gemakkelijk door kan geven.
- Recht op bezwaar: Betrokkene heeft het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens.
- Recht van verzet: Betrokkene heeft het recht aan de gemeente te vragen om zijn/haar persoonsgegevens niet meer te gebruiken.

Op hoofdlijnen zijn de rechten op grond van de Wpg gelijkluidend aan die van de AVG. Op een aantal punten verschilt dit. Betrokkenen kunnen met betrekking tot Wpg-gegevens de volgende verzoeken/bezwaren bij de gemeente doen:

- recht op informatie (Wpg art. 24);
- recht op inzage (Wpg art. 25);
- recht op rectificatie en/of aanvulling en/of vernietiging (Wpg art. 28).

De gemeente kan het verzoek m.b.t. politiegegevens (Wpg) van de betrokkene afwijzen als:

- Het gerechtelijke onderzoeken of procedures zou belemmeren.
- Dat nadelige gevolgen heeft voor het voorkomen van het begaan van strafbare feiten, voor opsporing, onderzoek, vervolging of het opleggen van straffen.
- De openbare veiligheid in het geding is.

- De rechten en vrijheden van derden worden geschonden.
- De nationale veiligheid in het geding is.

Een verzoek kan ook worden afgewezen als het kennelijk een ongegrond of buitensporig verzoek is.

Bij een inzageverzoek op basis van de Wpg verstrekt de gemeente geen documenten, maar stelt de betrokkene in de gelegenheid om op inzage te komen. Hierbij mogen geen foto's en of kopieën gemaakt worden van deze afschriften. In het besluit wordt opgenomen welke gegevens de gemeente Bergen geregistreerd heeft (Wpg art. 29 lid 5).

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 gedefinieerd, 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. De gemeente borgt dit met automatisering en een eigen werkinstructie.

Het ter beschikking stellen 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.

Doorgifte van persoonsgegevens
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waaraan de gegevensuitwisseling moet voldoen. Deze afspraken worden door de gemeente vastgelegd in overeenkomsten en zijn overeenkomstig wet- en regelgeving. De gemeente kan voor het uitoefenen van haar taken de verwerking van persoonsgegevens uitbesteden aan verwerkers. Daarbij maakt de gemeente alleen gebruik van verwerkers die voldoende technische en organisatorische maatregelen hebben getroffen en zodoende voldoen aan de AVG en Wpg vereisten.

Het kan zijn dat de gemeente met een andere partij gezamenlijk verwerkingsverantwoordelijke is, bijvoorbeeld door een samenwerking aan te gaan met een andere gemeente. In dat geval sluit de gemeente een overeenkomst af waarin de verplichtingen en verantwoordelijkheden voor beide partijen zijn opgenomen.

In het register van verwerkingsactiviteiten van de gemeente is per verwerking inzichtelijk of de persoonsgegevens zijn gedeeld met derden, hoe deze derden worden gekwalificeerd en of hiermee een overeenkomst is aangegaan. Voorafgaand aan iedere doorgifte voert de privacy officer een controle uit op de kwalificatie van partijen en de overeenkomst. De privacy officer controleert de overeenkomsten en de daarin vastgestelde afspraken jaarlijks.

Met betrekking tot doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (EER), geldt het uitgangspunt dat de persoonsgegevens niet worden doorgegeven. Dit uitgangspunt is niet van toepassing op een aantal derde landen, of sectoren binnen die landen, waarvoor een adequaatheidsbesluit is genomen door de Europese Commissie (EC). De EC geeft daarmee aan dat deze landen een passend beschermingsniveau van persoonsgegevens waarborgen conform de AVG. Voorts kan de doorgifte van persoonsgegevens naar landen/organisaties buiten de EER plaatsvinden indien een

wettelijke uitzondering of een rechtmatig overdrachtsmechanisme zoals omschreven in de AVG van toepassing is. Voornoemde doorgifte zal iedere keer binnen de voorwaardelijke kaders van wet- en regelgeving plaatsvinden.

Het melden van datalekken

De gemeente Bergen heeft in haar privacybeleid een procedure datalekken vastgesteld. Deze procedure heeft betrekking op de afhandeling van datalekken op grond van zowel de AVG als de Wpg.

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 Boa moet daarom verplicht jaarlijks een Wpg-awareness-sessie of Wpg e-learning module volgen. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog.

Functionaris gegevensbescherming (FG)

Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van een Functionaris Gegevensbescherming (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 taken van de FG (artikel 36 van de Wet politiegegevens) met betrekking tot de Wpg kunnen als volgt worden samengevat. De FG voert periodiek controles uit op het naleven van de wettelijke verplichtingen die voortkomen uit de Wpg, waaronder de controle op:

1. het beleid voor de uitvoering van de Wpg;
2. de bewustwordingsverplichting;
3. het autorisatieproces met betrekking tot het vastleggen van politiegegevens;
4. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
5. het verwerken van politiegegevens;
6. de bewaartermijnen;
7. het ter beschikking stellen en verstrekken van politiegegevens;
8. de informatiebeveiliging en het uitvoeren van een risicoanalyse;
9. de gegevensbeschermingseffectbeoordelingen (DPIA);
10. het register voor verwerkingen;
11. de verplichtingen ten aanzien van de audit;
12. het beoordelen van de DPIA's

Daarnaast is het de taak van de FG om samen te werken met de Autoriteit Persoonsgegevens en op te treden als contactpunt voor de Autoriteit Persoonsgegevens inzake aangelegenheden in verband met de verwerking van persoonsgegevens en indien nodig overleg te plegen. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

Het college van burgemeester en wethouders zal een Functionaris Gegevensbescherming (FG) aanstellen voor de Wpg. De FG houdt vanuit een onafhankelijke positie intern toezicht op de omgang met privacy en naleving van de Wpg door de gemeente Bergen.

Periodieke evaluatie van beleid

Dit aanvullend privacybeleid wordt minimaal één keer per jaar getoetst, of eerder indien nodig vanwege strategische ontwikkelingen, ontwikkelingen in de samenleving of verplichtingen voortvloeiend uit wet- en regelgeving. De wijzigingen van het privacybeleid worden nauwkeurig bijgehouden. Dit maakt monitoring en naleving van de vereisten zowel jaarlijks als ad-hoc mogelijk.

Inwerkingtreding

Dit aanvullend privacybeleid treedt in werking na vaststelling door het college van burgemeester en wethouders.