gemeente BERGEN Limburg

GEMEENTEBLAD

Officiële uitgave van de gemeente Bergen (L)

Nr. 470744

8 november 2024

Privacybeleid AVG en Wpg

Inleiding
Gemeente Bergen is zich ervan bewust dat privacy een belangrijke rol speelt in de relatie tussen de burger en de overheid. Privacy staat daarom hoog op onze bestuurlijke agenda. De gemeente heeft de verantwoordelijkheid over persoonsgegevens die zij verwerkt en uitwisselt met derde partijen. De gemeente ziet het als haar verplichting om zorgvuldig, veilig, proportioneel en vertrouwelijk om te gaan met persoonsgegevens die zij verwerkt. Het beschermen van persoonsgegevens is complex en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om binnen de gemeente duidelijk beleid te hebben over de omgang met persoonsgegevens en privacy.

In dit privacybeleid staat uiteengezet hoe de gemeente omgaat met persoonsgegevens die worden verwerkt en hoe de gemeente voldoet aan de Algemene verordening gegevensbescherming (AVG) en Wet politiegegevens (Wpg). Per onderwerp wordt aangegeven hoe aan de AVG en Wpg wordt voldaan.

Door de komst van de Algemene verordening gegevensbescherming (AVG) in 2018 hebben organisaties die persoonsgegevens verzamelen en gebruiken meer verantwoordelijkheden gekregen. En de mensen van wie zij gegevens gebruiken hebben meer rechten gekregen. De AVG bevat gedetailleerde voorschriften voor bedrijven en organisaties over het verzamelen, opslaan en beheren van persoonsgegevens.

Persoonsgegevens die een Boa verwerkt in zijn rol als toezichthouder, bijvoorbeeld bij een inspectie, vallen onder de AVG. Maar, de gegevens die de Boa als opsporingsambtenaar verwerkt, bijvoorbeeld het controleren van iemands identiteit als hij een verdachte aanhoudt of boetes uitdeelt, vallen onder de Wpg.

Naast dit privacybeleid is de gemeente in het bezit van een privacyreglement voor werknemers. Het privacyreglement is opgesteld voor alle werknemers en personen die werkzaamheden verrichten voor of namens de gemeente. Dat reglement bevat regels over de omgang met persoonsgegevens. Werknemers van de gemeente dienen zich tijdens hun dagelijkse werkzaamheden te houden aan de regels die daarin staan. Het privacyreglement is overzichtelijk en praktisch gehouden, zodat het voor alle werknemers duidelijk is wat van hen wordt verwacht.

1. Reikwijdte en wettelijke kaders

Dit privacybeleid is een uitwerking van de AVG en Wpg en beschrijft de naleving van de AVG en Wpg door de gemeente Bergen. De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens [ook die voor de verwerking van politiegegevens worden gebruikt] door of namens de gemeente, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente Bergen;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente Bergen aan een rechtspersoon die voor de gemeente Bergen bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:
- de Algemene Verordening Gegevensbescherming (AVG);
- de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
- het Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een DPIA verplicht is, Autoriteit Persoonsgegevens (AP);
- De Europese Verordening;
- 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;

Voor onze boa's is **ook** deze wet- en regelgeving relevant:
- de Wet politiegegevens (Wpg);
- het Besluit politiegegevens (Bpg);

- het Besluit politiegegevens buitengewoon opsporingsambtenaren.
- Interne beleidskaders en werkinstructies;

2. Doeleinden

Doel van het privacybeleid is te verduidelijken welke uitgangspunten worden gehanteerd bij het op een verantwoordelijke wijze omgaan met persoonsgegevens.
De gemeente Bergen wil onder andere bereiken dat:
- de basis voor een goed geïmplementeerd beleid op het gebied van privacy wordt gegarandeerd en dat alle medewerkers zich ten volle bewust zijn van de noodzakelijkheid van een zorgvuldige omgang met persoonsgegevens;
- De verwerking van persoonsgegevens moet ook 'behoorlijk' zijn. Dat betekent die niet (op een niet te rechtvaardigen manier) nadelig, discriminerend, onverwacht of misleidend mag zijn voor de betrokkenen
- de rechten van betrokkenen worden gerespecteerd/gewaarborgd en in procedures zijn verankerd;
- het vertrouwen van betrokkenen in de overheid niet wordt beschaamd;
- het beleid in lijn is met de relevante nationale en Europese wet- en regelgeving;
- uitvoering van het privacybeleid binnen de gemeente integraal en gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- de kans op financiële schade door het oplopen van boetes en reputatieschade wordt geminimaliseerd.

Het beleid is van toepassing op alle taken en processen waarvoor de gemeente Bergen verantwoordelijk is.

Naast dit privacybeleid is de gemeente Bergen in het bezit van een privacyreglement voor medewerkers. Het privacyreglement is opgesteld voor alle medewerkers en personen die werkzaamheden verrichten voor of namens de gemeente. Dat reglement bevat regels over de omgang met persoonsgegevens. Medewerkers van de gemeente dienen zich tijdens hun dagelijkse werkzaamheden te houden aan de regels die daarin staan. Het privacyreglement is overzichtelijk en praktisch gehouden, zodat het voor alle medewerkers duidelijk is wat van hen wordt verwacht. Het Privacyreglement is als addendum aan dit beleidsdocument toegevoegd.

Verantwoordelijkheid van iedere werknemer
Iedereen werkzaam binnen de gemeente Bergen is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar werknemers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

3. Principes voor de verwerking van persoonsgegevens

De AVG en Wpg zijn gebaseerd op een aantal principes voor de verwerking van persoonsgegevens c.q. politiegegevens. De gemeente Bergen onderschrijft deze principes en stelt zich ten doel persoonsgegevens c.q. politiegegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag
Persoonsgegevens worden door de gemeente Bergen slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een publiekrechtelijke taak.

Welbepaalde doeleindbing
De gemeente Bergen verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

Verdere verwerking
Persoonsgegevens op basis van de AVG kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente Bergen voert, voordat de andere/af-

geleide verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente Bergen bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

De gemeente Bergen verwerkt politiegegevens alleen als daar een doel en een wettelijke grondslag voor is. Alleen de BOA's van Domein I en Domein II van de gemeente Bergen verzamelen en verwerken deze gegevens. Gemeente Bergen verwerkt politiegegevens uitsluitend op basis van artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak door BOA's) en op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (artikel 15-21 en 23-24 Wpg). De gemeente Bergen verwerkt geen politiegegevens als bedoeld in de artikelen 9, 11 en artikel 13 Wpg (dus geen onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval, geautomatiseerde vergelijkingen en ondersteunende taken).

Politiegegevens worden slechts verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

Juiste en actuele gegevens
De gemeente Bergen zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen. Daarnaast is het voor betrokkenen mogelijk om bij de gemeente een verzoek in te dienen op rectificatie, aanvulling of vernietiging van politiegegevens.

Bewaartermijnen: gegevens worden op tijd vernietigd
De gemeente Bergen stelt de bewaartermijn van een verwerking in het kader van de AVG en Wpg vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Binnen gemeente Bergen worden politiegegevens niet langer bewaard dan noodzakelijk, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Alle politiegegevens worden opgeslagen in een speciaal daarvoor bedoeld systeem dat automatisch de bewaartermijnen waarborgt.

Integriteit en vertrouwelijkheid
De gemeente Bergen neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design
De gemeente Bergen houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente Bergen geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. Met technische en organisatorische maatregelen de beginselen uit de AVG, zoals de vertrouwelijkheid van gegevens, moet dat worden nageleefd.
Aan de regels uit de AVG moeten worden voldaan en moeten de rechten van betrokkenen worden beschermd.

Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente Bergen, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen.

Datalekken worden binnen gemeente altijd gemeld aan de Functionaris gegevensbescherming. De gemeente heeft een procedure opgesteld voor het aanpakken en afhandelen van datalekken. De procedure is gedocumenteerd in het Protocol datalekken. Daarin staat de specifieke afhandeling van datalekken binnen de gemeente. Deze procedure is naar alle werknemers toe gecommuniceerd. Alle werknemers zijn op de hoogte van de procedure. Wanneer werknemers de procedure willen nalezen, dan kunnen zij de procedure gemakkelijk terugvinden op het intranet. De datalekkenprocedure is altijd beschikbaar voor werknemers.

Alle werknemers van gemeente Bergen hebben een presentatie gekregen over datalekken. Daarin hebben zij geleerd hoe zij incidenten en datalekken kunnen herkennen en wat zij dienen te doen wanneer zij een incident of datalek vermoeden.

Binnen de gemeente is er een Datalek Team opgericht dat datalekken beoordeelt en afhandelt. Het Datalek Team bestaat uit:
1. Gemeentesecretaris
2. Functionaris gegevensbescherming (FG)
3. Privacy Officer (PO)
4. Adviseur informatiebeveiliging (Chief Information Security Officer)

De gemeente voert een bemoedigingsbeleid voor het melden van incidenten en datalekken. Elk incident en datalek wordt geregistreerd in TOPdesk. Datalekken worden altijd geëvalueerd en indien dat noodzakelijk is, treft gemeente maatregelen aan de hand van de evaluatie.

Samenwerking
Voor de uitoefening van haar taken en verantwoordelijkheden werkt de gemeente Bergen samen met partners buiten de organisatie van de gemeente. Dat kunnen andere overheidsinstanties zijn, maar het zijn soms ook private partijen. Partijen die als verwerker worden aangemerkt, zullen uitsluitend in opdracht en ten behoeve van de gemeente optreden. De gemeente draagt er zorg voor dat met deze partijen duidelijke afspraken worden gemaakt, zogenaamde verwerkersovereenkomsten. Een lijst van verwerkersovereenkomst wordt in het DMS van Bergen(L) vastgelegd. Deze afspraken zijn afgestemd op de geldende wet- en regelgeving. Daarbuiten verstrekt de gemeente persoonsgegevens alleen aan derden voor zover dit noodzakelijk is voor een goede uitvoering van onze taken en verantwoordelijkheden en voor zover dit verplicht is op grond van de wet.

Samenwerkingsverbanden
Verder kan het voorkomen dat de gemeente Bergen samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie
De gemeente Bergen informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten

en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen
Onder de AVG en Wpg hebben betrokkenen een aantal rechten om grip op hun persoonsgegevens te houden. Gemeente Bergen heeft deze rechten in haar privacyverklaring gezet. De privacyverklaring is terug te vinden op de website www.bergen.nl. De gemeente heeft betrokkenen zowel de mogelijkheid gegeven om dit formulier via de e-mail in te dienen als op papier in te leveren bij het Klant Contact Centrum van de gemeente. Wanneer de gemeente een verzoek ontvangt van een betrokkene dan handelt zij dit verzoek binnen één maand af. Hoe een verzoek wordt behandeld en afgehandeld staat beschreven in de "Procedure verzoeken betrokkenen" van de gemeente Bergen.

Geschillenbeslechting
Indien de betrokkene van mening is dat de gemeente Bergen niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente Bergen over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG en Wpg intern worden nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister
De gemeente Bergen beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Functionaris gegevensbescherming (FG)
Gemeente Bergen is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan het MT, de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

Gemeente Bergen heeft een FG aangesteld. Deze persoon is aangemeld bij de Autoriteit Persoonsgegevens. De FG houdt toezicht op de verwerking van persoonsgegevens en houdt toezicht op de naleving van de AVG en Wpg door gemeente Bergen. Naast een FG heeft de gemeente ook een Privacy Officer. Deze persoon heeft naast de FG ook taken op het gebied van privacy en de omgang met persoonsgegevens binnen de organisatie.

PDCA Cyclus
De gemeente Bergen streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en aantoonbaar worden uitgevoerd ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel proces verankerd is in een Plan-Do-Check-Act-cyclus.

Gemeente Bergen maakt gebruik van een ISMS systeem voor het waarborgen van privacy compliance binnen de gemeente.

Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

Data Protection impact assessment (DPIA)

Gemeente Bergen voert DPIA's uit waar nodig is. Hiervoor heeft de gemeente een protocol opgesteld: "Protocol Data Protection Impact Assessment". Daarin staat wat een DPIA is, wanneer een DPIA verplicht is en wat de procedure is bij de gemeente omtrent de DPIA. Op basis van uitkomsten van de DPIA onderneemt de gemeente gerichte acties om de bestaande risico's zo veel mogelijk te verminderen.

4. Rollen en Verantwoordelijken

College van B&W
Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente Bergen. Het College heeft de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente Bergen;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

Afdelingshoofden en directeuren
De algemeen directeur en de afdelingsmanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.

De algemeen directeur en afdelingsmanagers hebben de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevordert duurzame privacycultuur;
- Betrekt PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)
Op basis van de AVG en de Wpg is het aanstellen van een FG verplicht voor de gemeente Bergen. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG en Wpg. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:
- Interne toezichthouder op de naleving van de AVG en Wpg namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Rapporteert en adviseert aan het college van burgemeester en wethouders over het jaarplan voor de Wpg;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie) en controleert op de compliance met de AVG en Wpg door middel van controles;
- Met het oog op de controle op de naleving van de regels van de Wpg worden ten minste de volgende controletaken en toezichtmaatregelen (TZM) uitgevoerd:
- Toezichtmaatregelen (TZM):
    1. Norm 2: Jaarlijks Toezicht van de FG op de doelbinding.
    2. Norm 3: Controles op de noodzakelijkheid en rechtmatigheid door de FG (of PO).
    3. Norm 4: Controles op het vernietigen en rectificeren van politiegegevens.

4. Norm 6: Controles op uitvoering DPIA's.
5. Norm 28: Beschikbaarheid logbestanden.
6. Norm 29: Planning, uitvoering en rapportage van de interne audits.
7. Norm 31: Overige toezichttaken van de FG.

Privacy Officer
De Privacy Officer is het eerste aanspreekpunt voor de gemeente Bergen rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van DPIA's en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Chief Information Security Officer (CISO)
Definieert het informatiebeveiligingsbeleid, gebaseerd op een risicomanagement-benadering en rekening houdend met het informatiebeveiligingsdreigingsbeeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en de inzet hiervan op concrete beveiligingsmaatregelen. Initieert en coördineert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.

Is verantwoordelijk voor:

- Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen

- Het inrichten van de informatiebeveiligingsorganisatie
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten
- Afstemming van informatiebeveiliging met andere beveiligingsdomeinen
- Het toezien op naleving van de eisen voor informatiebeveiliging
- Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie
- De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten
- Het adviseren bij en begeleiden van informatierisicoanalyses
- Het uitvoeren van informatiebeveiligingsassessments

Realiseert:
- Organisatiebrede informatiebeveiligingsactiviteiten en -projecten
- Monitoring van de relevante risico's voor de organisatie
- Monitoring van compliance met beleid en wet- en regelgeving
- Gecoördineerde reactie op ernstige informatiebeveiligings- of ICT- incidenten
- Organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatie- beveiliging

5. Slotwoord

Dit privacybeleid is opgesteld met het oog op het hebben van een duidelijk beleid ten aanzien van de omgang met persoonsgegevens binnen de gemeente Bergen. De gemeente werkt er constant aan om persoonsgegevens te beschermen op een manier die passend is voor de situatie. De gemeente zal haar processen en protocollen dan ook periodiek (elke 2 jaar) - of eerder bij (grote) wijzigingen met grote inpact - evalueren en aan de hand daarvan updaten.

Dit privacybeleid treedt in werking na vaststelling door B&W van de gemeente Bergen (L).