Gemeente Bergen op Zoom

GEMEENTEBLAD

Officiële uitgave van de gemeente Bergen op Zoom

Nr. 284668

29 juni

2023

Beleidsregel van het college van burgemeester en wethouders van Bergen op Zoom inhoudende Privacybeleid gemeente Bergen op Zoom

Privacybeleid

Vastgesteld op: 30 mei 2023

Inleiding

Binnen de gemeente Bergen op Zoom wordt veel gewerkt met persoonsgegevens van burgers, ondernemers, medewerkers en partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. Bijvoorbeeld op het gebied van burgerzaken, openbare orde en veiligheid en zorg en inkomen. De gemeente is daarbij wettelijk verplicht om zorgvuldig en veilig met deze persoonsgegevens om te gaan en de mensen moeten hierop ook kunnen vertrouwen.

Technologische en juridische ontwikkelingen, de globalisering en uitdagingen op het gebied van bijvoorbeeld zorg en veiligheid maken het beschermen van gegevens daarbij vaak complex. De gemeente is zich hiervan bewust en vindt het belangrijk om de bescherming van gegevens zo goed mogelijk te waarborgen en ook transparant te zijn over de manier waarop zij met persoonsgegevens omgaat.

Het gaat er ook om de juiste technische maatregelen te treffen op het gebied van beveiliging. Maar vooral de mensen van de organisatie, dus het bestuur, management en alle medewerkers en de mate waarin zij bewust zijn van risico's en veilig gedrag spelen hierbij een cruciale rol.

Met dit beleid wil de gemeente dan ook voor iedereen duidelijk richting geven aan de manier waarop zij de privacy van mensen wil waarborgen, beschermen en handhaven. Dit beleid beschrijft daarom welke uitgangspunten binnen de gemeente gelden met betrekking tot de bescherming van privacy. Dit beleid is van toepassing op de hele organisatie en op alle verwerkingen van persoonsgegevens door of namens de gemeente.

1. Wettelijk kader en definities

Grondrechten op privéleven en het recht op bescherming van persoonsgegevens zijn vastgelegd in artikel 16 van het Verdrag betreffende de werking van de Europese Unie, artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie, artikel 8 Europees Verdrag voor de Rechten van de Mens en artikel 10 van de Nederlandse Grondwet.

Daarbij regelt de Europese Algemene Verordening Gegevensbescherming (AVG) samen met de Nederlandse Uitvoeringswet (UAVG), het algemeen juridisch kader voor de omgang met persoonsgegevens.

De AVG is van toepassing op "de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen". Dit betekent kort gezegd dat de AVG van toepassing is op nagenoeg iedere verwerking van persoonsgegevens, zowel digitaal als op papier.

Daarnaast zijn er specifieke regels voor de verwerking van persoonsgegevens door gemeentelijke boa's in het kader van opsporingstaken. Die verwerkingen vallen niet onder de AVG maar onder de Wet politiegegevens (Wpg). De AVG en de Wpg sluiten elkaar onderling uit maar kennen ook veel overlap. Net als de AVG verplicht de Wpg bijvoorbeeld tot het treffen van beveiligingsmaatregelen, het bijhouden van een register, het afsluiten van verwerkersovereenkomsten, het melden van datalekken, het voorzien in de rechten van betrokkenen, het aanstellen van een FG en het uitvoeren van DPIA's. De hiervoor vastgestelde procedures worden dan ook voor zowel de AVG als de Wpg toegepast en kennen slechts verschillen bij de inhoudelijke uitwerking. Dit privacybeleid kan dan ook met name worden beschouwd als een uitwerking van de AVG en de Wpg.

Voor de definitie van begrippen wordt verwezen naar artikel 4 AVG en artikel 1 Wpg. Voor de duidelijkheid wordt hieronder een korte omschrijving gegeven van enkele belangrijke en veel voorkomende begrippen:

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is dus degene van wie de gegevens worden verwerkt.

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals gezondheidsgegevens, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, woonplaats, e-mail, geboortedatum, burgerservicenummer enzovoort).

Bijzondere persoonsgegevens: Naast gewone persoonsgegevens kent de wet zogenaamde bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen. Omdat de verwerking ervan veel impact kan hebben op iemands leven, worden bijzondere persoonsgegevens extra beschermd. Bijzondere persoonsgegevens zijn gegevens over ras, etnische afkomst, politieke opvattingen, godsdienst, lidmaatschap van een vakbond, genetische en biometrische gegevens, gezondheid, seksuele gerichtheid en strafrechtelijke gegevens.

Politiegegevens: Een persoonsgegeven dat wordt gebruikt voor verwerking in het kader van de opsporingstaak. Een politiegegeven is dus een specifieke versie van een persoonsgegeven. Daar waar in dit beleid wordt gesproken over persoonsgegevens wordt tevens bedoeld politiegegevens in de zin van de Wpg.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, raadplegen, verstrekken aan een ander en vernietigen.

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Hiervoor wordt meestal de afkorting DPIA gebruikt. Dit verwijst naar de Engelse term Data Protection Impact Assesment.

Naast het algemeen juridisch kader uit de AVG en de Wpg zijn er nog verschillende sectorspecifieke wetten die voor de overheid nadere regels geven voor het verwerken van persoonsgegevens. Belangrijke voorbeelden zijn in dit verband de Wet basisregistratie personen (Brp), de Participatiewet (Pw), de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet (Jw). Bij de uitvoering van deze sectorspecifieke wetten gaan de bijzondere regels uit deze wetten vóór op de algemene regels uit de AVG

en/of de Wpg. Daar waar niets in de sectorspecifieke wetgeving is geregeld, blijft de AVG en/of de Wpg van toepassing.

2. Kernwaarden, uitgangspunten en grondslagen

2.1 Kernwaarden organisatie

De kernwaarden die voor de gemeente leidend zijn bij de sturing van de organisatie zijn uitgewerkt in de Sturingsfilosofie 2022. Ten aanzien van houding en gedrag zijn de volgende kernwaarden vastgesteld:
1. Dienstbaar (de waarde voor klanten voorop)
2. Integraal werkend (verbinden van domeinen en vraagstukken)
3. Betrouwbaar (je weet wat je aan ons hebt)
4. Betrokken (we leveren toegevoegde waarde)
5. Vooruit (we willen presteren en bij de beste gemeenten horen)
6. Voor elkaar (samenwerken, effectief, efficiënt en wendbaar)

Vertaald naar de omgang met persoonsgegevens betekent dit onder meer het volgende:

De gemeente verwerkt bij de uitvoering van haar publiekrechtelijke taken veel persoonsgegevens. De persoonsgegevens worden door betrokkenen vaak vrijwillig maar soms ook verplicht afgestaan. De gemeente is daarbij wettelijk verplicht zorgvuldig en veilig met deze persoonsgegevens om te gaan. Het zorgvuldig en veilig omgaan met de persoonsgegevens is tegelijkertijd een belangrijke waarde voor de organisatie. De burger moet er immers op kunnen vertrouwen dat gegevens bij de gemeente in veilige handen zijn en zorgvuldig en vertrouwelijk worden behandeld.

Daarbij moeten processen werkbaar worden gehouden en optimale dienstverlening worden geboden aan inwoners, bedrijven en andere betrokkenen. Vooral het professioneel, integer en transparant handelen van medewerkers vormt de basis om steeds een passende mate van gegevensbescherming te bieden zonder dat dit in de weg staat aan een goede en tijdige uitvoering van taken. Met name op bijvoorbeeld het gebied van zorg, openbare orde en veiligheid mag de uitvoering niet dusdanig ingewikkeld of rigide zijn dat het in weg staat aan effectief optreden van de gemeente.

Professioneel, integer en transparant handelen is vastgelegd in integriteitsbeleid. Alle medewerkers zijn op grond hiervan gehouden zorgvuldig en vertrouwelijk met persoonsgegevens om te gaan en steeds open te zijn over hun handelwijze. Daarbij neemt iedereen zijn verantwoordelijkheid voor zijn handelen. Dit kan door tijdig en adequaat te reageren op verzoeken van betrokkenen en deze waar nodig integraal op te pakken maar ook door proactief te handelen als de situatie daarom vraagt. Bijvoorbeeld door bij een datalek snel te handelen om gevolgen te beperken en herhaling te voorkomen of door actie te ondernemen waar regelgeving tekort schiet maar wel zaken geregeld moeten worden. Daarbij wordt erkend als zaken niet goed zijn gelopen zodat er kan worden geleerd van fouten en aan verbeteringen kan worden gewerkt.

2.2 Uitgangspunten

De verwerking van persoonsgegevens bij de gemeente moet plaatsvinden in overeenstemming met de privacy beginselen uit de AVG en Wpg[1]. Dit betekent dat de gemeente zich steeds houdt aan de volgende belangrijke uitgangspunten die direct uit de AVG en Wpg voortvloeien:

a. Rechtmatigheid, behoorlijkheid, transparantie
Persoonsgegevens worden alleen verwerkt als daarvoor een grondslag is in de wet. Bijvoorbeeld omdat de verwerking noodzakelijk is voor de uitvoering van een wettelijke taak. Daarbij worden betrokkenen zoveel mogelijk vooraf in duidelijke en eenvoudige taal geïnformeerd over de verwerking van persoonsgegevens. In het algemeen via bijvoorbeeld de algemene privacyverklaring op de website maar ook specifiek per verwerking via bijvoorbeeld aanvraagformulieren, brieven, folders en in gesprek.

b. Doelbinding

1) Artikel 5 lid 1 AVG en artikel 3, 4, 4a, 8, 9, 13 en 14 Wpg.

Persoonsgegevens worden alleen verwerkt voor vooraf bepaalde doelen en in de regel niet gebruikt voor een ander doel dan waarvoor ze zijn verkregen. Het gebruik van persoonsgegevens voor een ander doel kan alleen als dit verenigbaar is met het oorspronkelijke doel. Het doel geeft antwoord op de vraag 'waarom' persoonsgegevens worden verwerkt. Door de gemeente wordt het doel per verwerking vooraf en zo specifiek mogelijk geformuleerd en vastgelegd in het register van verwerkingen. Bij de uitvoering van publiekrechtelijke taken, bijvoorbeeld bij de uitvoering van de Wet basisregistraties personen of de Wet maatschappelijke ondersteuning, zijn voor de gemeente de doelen voor het verwerken in de regel al in de wet vastgelegd, evenals de persoonsgegevens die daarbij verwerkt mogen worden.

c. Dataminimalisatie
Er worden alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het vooraf bepaalde doel. Wanneer met minder of geen persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

d. Juistheid
Persoonsgegevens die worden verwerkt moeten juist zijn en zo nodig worden geactualiseerd.

e. Opslagbeperking
Persoonsgegevens worden niet langer bewaard dan nodig voor het doel of wettelijk verplicht. Wanneer er persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het doel en waarvoor geen wettelijke bewaartermijn is vastgesteld, worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Voor elke verwerking van persoonsgegevens worden bewaartermijnen vastgesteld en vastgelegd in het register van verwerkingen. Uitgangspunt bij het vaststellen van bewaartermijnen is de selectielijst op grond van de Archiefwet.[2]

f. Integriteit en vertrouwelijkheid
Persoonsgegevens worden veilig en vertrouwelijk behandeld. Persoonsgegevens worden bijvoorbeeld alleen verwerkt door personen die zijn gebonden aan geheimhouding. De geheimhoudingsplicht geldt voor ambtenaren op grond van de Ambtenarenwet en het Integriteitsbeleid. Door de gemeente ingehuurde derden verklaren schriftelijk en voorafgaand aan hun inzet zich te houden aan dezelfde regels. De wijze waarop persoonsgegevens worden beveiligd is verder vastgelegd in het Informatiebeveiligingsbeleid van de gemeente.

2.3 Wettelijke grondslagen

Een belangrijk uitgangspunt is dat persoonsgegevens rechtmatig worden verwerkt. Dat betekent dat er voor de verwerking van persoonsgegevens altijd een grondslag uit de wet van toepassing moet zijn.[3] De AVG kent zes grondslagen op basis waarvan persoonsgegevens mogen worden verwerkt:

a. de betrokkene heeft **toestemming**gegeven voor de verwerking van zijn persoonsgegevens;
Voorbeeld: Een betrokkene gaat akkoord met de verwerking van zijn e-mailadres voor het ontvangen van een nieuwsbrief.
b. de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is;
Voorbeeld: Bij de verkoop van een dienst of product worden gegevens verwerkt voor de levering en/of betaling.
c. de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting**;
Voorbeeld: Een werkgever is op grond van belastingwetgeving verplicht een kopie identiteitsbewijs van een werknemer te bewaren.
d. de verwerking is noodzakelijk om de **vitale belangen**van de betrokkene of een ander te beschermen;
Voorbeeld: Wanneer er acuut gevaar dreigt en iemand fysiek of mentaal niet in staat is om toestemming te geven voor hulp.
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (**uitvoering publieke taak**);
Voorbeeld: De gemeente verwerkt gegevens voor het uitvoeren van wettelijke taken zoals bij het aanvragen van een vergunning of uitkering.
f. de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen** van de gemeente of van een derde.

2) Op grond van de Archiefwet worden selectielijsten gemaakt waarin wordt beschreven welke informatie op welke termijn moet worden vernietigd en welke informatie permanent bewaard moet worden. Zie artikel 5 Archiefwet.
3) Artikel 6 lid 1 AVG en artikel 3 Wpg.

Voorbeeld: Het verwerken van gegevens om medewerkers, gebouwen of computersystemen te beveiligen.

Behalve voor 'toestemming' moet er voor alle grondslagen ook een 'noodzaak' zijn om persoonsgegevens te verwerken. En die noodzaak moet worden gemotiveerd. Het is dus niet voldoende dat kan worden verwezen naar het bestaan van een 'overeenkomst' of een 'publieke taak'. Er zal ook altijd moeten kunnen worden aangetoond dat het verwerken van persoonsgegevens 'noodzakelijk' is voor de uitvoering van de overeenkomst of publieke taak.

Voor taken die bij wet aan de gemeente zijn opgedragen vormt in de regel "de uitvoering van een publieke taak" de wettelijke grondslag voor de verwerking van persoonsgegevens. Bij de gemeente is dit bij verreweg de meeste verwerkingen het geval.

Voor zover persoonsgegevens worden verwerkt voor niet-wettelijke taken moet een andere grondslag kunnen worden aangewezen. Toestemming van de betrokkene is daarbij soms, maar niet altijd een alternatief voor de gemeente. Tussen de gemeente en de burger bestaat namelijk een bepaalde afhankelijkheidsrelatie, zodat niet altijd aan de eis kan worden voldaan dat toestemming 'vrijelijk' moet zijn gegeven. De grondslag gerechtvaardigd belang kan ook een alternatief zijn, maar mag alleen worden gebruikt voor zover dat gaat om typische bedrijfsmatige handelingen (waarbij de overheid zich niet onderscheidt van een private partij), bijvoorbeeld voor het instellen van cameratoezicht voor het beschermen van personeel en eigendom.

Voor zover persoonsgegevens door boa's worden verwerkt in het kader van de Wpg is sprake van strafrechtelijke handhaving. De grondslag volgt dan niet uit de AVG maar uit de Wpg. De grondslag is dan in de regel artikel 8 van de Wpg (**uitvoering van dagelijkse politietaak**).[4]

3. Privacy organisatie

3.1 Rollen en verantwoordelijkheden

De verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens ligt bij de afdelingen die werken met persoonsgegevens. Dit betekent dat intern de afdelingsmanagers worden aangesproken op het naleven van het privacybeleid. Privacy is immers niet een op zichzelf staand iets, maar onlosmakelijk verbonden met de gemeentelijke dienstverlening binnen de afdelingen.

In onderstaande paragrafen worden de verschillende rollen met bijbehorende verantwoordelijkheden binnen de organisatie benoemd. In bijlage 1 zijn de verantwoordelijkheden van de verschillende rollen bij een aantal belangrijke taken op het gebied van gegevensbescherming in onderling verband vastgelegd in een matrix.

3.1.1 Bestuur

De bestuursorganen van de gemeente zijn wettelijk eindverantwoordelijk voor de verwerkingen van persoonsgegevens die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn de burgemeester, het college van burgemeester en wethouders en de gemeenteraad. De burgemeester is verantwoordelijk voor de verwerkingen die te maken hebben met zijn veiligheidstaken. De gemeenteraad is verantwoordelijk voor de verwerkingen binnen de griffie en door de raad ingestelde commissies. Het college van burgemeester en wethouders is verantwoordelijk voor alle overige gegevensverwerkingen binnen de gemeente en daarmee voor het leeuwendeel van de gemeentelijke verwerkingen. Wanneer wordt gesproken over de 'verwerkingsverantwoordelijke' in de zin van de AVG, wordt bij de gemeente in de regel dan ook het college van burgemeester en wethouders bedoeld. In bijna alle gevallen speelt het college ook een rol bij de verwerkingen omdat de burgemeester en de gemeenteraad ook gebruik maken van de ambtelijke organisatie. In die zin zijn de verantwoordelijkheden op het gebied van gegevensbescherming moeilijk strikt te scheiden en met elkaar verbonden. Het col-

4) Er kan ook sprake zijn van een verwerking op grond van artikel 9 Wpg (verwerkingen gericht op bepaalde personen of gebeurtenissen) maar die vinden in de regel niet plaats bij de gemeente. Omdat bij een verwerking op grond van artikel 9 meer inbreuk wordt gemaakt op de privacy van betrokkenen geldt dat daarbij als extra waarborg een "bevoegd functionaris" moet worden aangewezen om toestemming te geven voor de verwerking en op de uitvoering toe te zien.

lege is dan ook verantwoordelijk voor het vaststellen van het privacybeleid voor de gemeentelijke organisatie en het stimuleren van het management om dit te volgen en waar nodig maatregelen te treffen om de persoonsgegevens van betrokkenen te beschermen. Het college heeft de verantwoordelijkheid voor de uitvoering van beleid opgedragen aan de gemeentesecretaris (algemeen directeur).

3.1.2 Gemeentesecretaris (algemeen directeur) en de griffie

De gemeentesecretaris is de hoogste ambtenaar binnen de organisatie en de eerste adviseur van het college. Hij vormt met het directieteam de schakel tussen het bestuur en de medewerkers. Hij is met het directieteam verantwoordelijk voor de juiste en volledige implementatie van de wet- en regelgeving op het gebied van privacy binnen de afdelingen. Daarvoor worden afdelingsmanagers als proceseigenaren aangewezen en gestimuleerd het privacybeleid te volgen.

Binnen de gemeentelijke organisatie neemt de griffie hierbij een aparte plaats in. De griffie verricht werkzaamheden voor de gemeenteraad en de griffier en de medewerkers van de griffie worden door de gemeenteraad benoemd. Er is dan ook geen gezagsverhouding met het college en de gemeentesecretaris in zijn rol van algemeen directeur van de gemeente. In de praktijk maakt de griffie wel gebruik van de ambtelijke organisatie. In de privacy organisatie wordt de griffie dan ook gelijkgesteld met een afdeling (als organisatieonderdeel waar verwerkingen van persoonsgegevens plaatsvinden) en de griffier met de gemeentesecretaris dan wel de afdelingsmanager (als proceseigenaar verantwoordelijk voor de bescherming van persoonsgegevens).

3.1.3 Proceseigenaar (lijnmanagement)

De verwerkingen van persoonsgegevens vinden operationeel plaats binnen de afdelingen van de organisatie. De afdelingsmanager is hierbij de proceseigenaar en daarmee verantwoordelijk voor de bescherming van de persoonsgegevens die door de afdeling worden verwerkt.[5] De afdelingsmanagers zijn daarmee verantwoordelijk voor het sturen op en monitoren van de uitvoering van het privacybeleid en het werken aan het privacy bewustzijn van de medewerkers. Zij zorgen ook voor het aanstellen van de contactpersonen privacy die hen op de afdeling ondersteunen in de dagelijkse naleving van de AVG.

<u>Belangrijke verantwoordelijkheden proceseigenaar:</u>
- Nieuwe verwerkingen of wijzigingen in bestaande verwerkingen van persoonsgegevens in vroeg stadium aanmelden bij de FG/PO voor toetsing aan beleid en opname in het register van verwerkingen;
- Het in behandeling nemen van verzoeken voor de uitoefening van privacyrechten (bijvoorbeeld verzoek om inzage, correctie of verwijdering) ten aanzien van persoonsgegevens die door de afdeling worden verwerkt;
- Het uitvoeren van DPIA's en het zo nodig uitvoeren van de maatregelen naar aanleiding van een DPIA;ec
- Het afsluiten, beheren en actualiseren van verwerkers- en andere privacyovereenkomsten;
- Het aanwijzen van een contactpersoon informatieveiligheid en privacy voor de afdeling;
- Het intern melden en afhandelen van datalekken binnen de afdeling, waaronder de uitvoering van adviezen van het datalekteam;
- Waar nodig het privacybeleid verder uitwerken in domein-, afdelings- of processecifieke richtlijnen of instructies.
- Het belang van informatieveiligheid en privacy periodiek onder de aandacht brengen van de afdeling.

3.1.4 CISO

De verwerking van persoonsgegevens is onlosmakelijk verbonden met de beveiliging daarvan. Beveiliging van persoonsgegevens is een verantwoordelijkheid van iedere medewerker. Maar om er voor te zorgen dat er een samenhangend pakket aan maatregelen in de gemeente beschikbaar is ter waarborging van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie binnen een gemeente is er de CISO; Chief Information Security Officer. De CISO houdt in samenwerking met de FG en de Privacy Officer (PO) toezicht op en adviseert over de beveiliging van persoonsgegevens binnen de organisatie. De verantwoordelijkheden van de CISO zijn vastgelegd bij het Informatiebeveiligingsbeleid, laatstelijk vastgesteld in 2021 (IB-beleid 2021-2024).

<u>Belangrijke verantwoordelijkheden CISO:</u>
- Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;

5) Inclusief de verwerking van persoonsgegevens in processen die daarbij namens de gemeente worden uitgevoerd door een leverancier of samenwerkingsverband.

• 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 voor de hele organisatie;
• De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's;
• Het adviseren bij en begeleiden van informatierisicoanalyses;
• Het uitvoeren van informatiebeveiligingsassessments;
• Het ondersteunen van de afdelingsmanagers bij het beheersen van risico's en het treffen/borgen van maatregelen.

3.1.5 Functionaris Gegevensbescherming FG

De AVG en de Wpg stellen een Functionaris Gegevensbescherming (FG) verplicht voor overheidsinstanties.[6] De FG heeft tot taak om onafhankelijk toezicht te houden op de naleving van privacywetgeving. Daarnaast zijn de taken van de FG het informeren en adviseren van de organisatie over de toepassing van privacywetgeving en optreden als contactpersoon van de Autoriteit Persoonsgegevens en burgers met vragen over privacy. De wet en het beleid zien op alle verwerkingen van persoonsgegevens en daarmee dus ook op de verwerking van de gegevens van de medewerkers van de gemeente. De FG houdt dus ook toezicht op die verwerkingen en medewerkers kunnen voor vragen hierover ook direct bij de FG terecht. Voor het uitoefenen van toezicht heeft de FG controlebevoegdheden. De FG neemt geen taken op het gebied van gegevensbescherming over van de afdelingen. De afdelingen hebben hierin hun eigen verantwoordelijkheid. Een nieuw proces of een wijziging van een bestaand proces waarbij persoonsgegevens worden verwerkt moeten door de afdelingen wel altijd vooraf bij de FG worden gemeld. De FG kan zo zijn verantwoordelijkheid nemen om deze te toetsen aan de wettelijke eisen en het gemeentelijk beleid op het gebied van privacy en de afdeling hierover adviseren. De FG rapporteert rechtstreeks aan de gemeentesecretaris/directie en het college van B&W.

<u>Belangrijke verantwoordelijkheden FG:</u>
• Informeren en adviseren van de gemeente en verwerkers voor de gemeente over hun verplichtingen volgens de AVG en de Wpg en andere wet- en regelgeving omtrent gegevensbescherming;
• Toezien op naleving van de AVG en de Wpg en andere wet- en regelgeving omtrent gegevensbescherming;
• Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
• Ontwikkelen en onderhouden van het algemeen gemeentelijk privacybeleid en adviseren en ondersteunen bij het opstellen van interne regelingen op het gebied van privacy;
• Beheer van het register van verwerkingen voor de gemeente;
• Advisering bij beveiligingsincidenten en het beheer van het werkproces voor het melden van datalekken waarbij persoonsgegevens betrokken zijn alsmede het beheer van het register van
• Adviseren met betrekking tot DPIA's en het toezien of de uitvoering daarvan in overeenstemming is met de AVG en de Wpg;
• Toezien op en adviseren over de afhandeling van vragen en klachten over het gebruik van persoonsgegevens;
• Samenwerken met en als contactpunt optreden voor de Autoriteit Persoonsgegevens en tevens fungeren als contactpersoon voor betrokkenen over aangelegenheden die verband houden met de verwerking van hun gegevens.

3.1.6 Privacy Officer (PO)

De gemeente heeft naast de FG een Privacy Officer (PO) aangewezen. Deze vormt een belangrijk onderdeel van de privacyorganisatie binnen de gemeente. De PO beschikt over kennis voor wat het betreft het toepassen van privacywetgeving in de praktijk en kan de organisatie ondersteunen bij de toepassing op casusniveau en de inrichting van processen en systemen. De PO richt zich dus op de uitvoering en is bijvoorbeeld betrokken bij het opstellen van verwerkersovereenkomsten en DPIA's en bij de behandeling van dataleken en verzoeken van betrokkenen in het kader van de AVG en de Wpg. Door deze uitvoerende taken bij de PO te beleggen wordt de FG primair in staat gesteld zijn adviserende en toezichthoudende rol te vervullen.

<u>Belangrijke verantwoordelijkheden van de PO:</u>
• Het adviseren en ondersteunen van de organisatie bij de toepassing en naleving van het privacybeleid;

6) Artikel 37 t/m 39 AVG en artikel 36 Wpg.

• De inhoudelijke advisering en ondersteuning van de organisatie bij het aangaan van verwerkers- en andere privacyovereenkomsten;
• Het adviseren bij en coördineren van de afhandeling van datalekken;
• De behandeling van AVG- en Wpg-verzoeken (om bijvoorbeeld inzage, correctie of verwijdering) en/of de coördinatie hiervan in de organisatie;
• Het initiëren en begeleiden van de uitvoering van DPIA's;
• Het adviseren van de organisatie bij de inrichting of wijziging van de bedrijfsvoering en processen (bijvoorbeeld bij de implementatie van maatregelen in het kader van een DPIA of Privacy by Design en Privacy by Default);
• Het beheer van het register van verwerkingen en het register van datalekken in samenspraak met de FG;
• Bijdragen aan het vergroten van het privacybewustzijn binnen de organisatie.

3.1.7 Contactpersonen informatiebeveiliging en privacy

Het uitgangspunt is dat er een contactpersoon informatiebeveiliging en privacy wordt aangewezen per afdeling of vakgroep en in ieder geval door iedere afdelingsmanager minimaal één contactpersoon wordt aangewezen. De contactpersoon kan de afdelingsmanager ondersteunen bij de naleving van het privacybeleid. De afdelingsmanager blijft als proceseigenaar verantwoordelijk voor zorgvuldige en veilige verwerking van persoonsgegevens binnen de afdeling. De contactpersoon privacy wordt geacht inhoudelijk bekend te zijn met het privacybeleid en is binnen het team aanspreekpunt voor advies over de verwerking van persoonsgegevens en de uitleg van de AVG en de Wpg. De contactpersoon privacy is voor de afdeling ook de eerste schakel naar de FG, de PO en de CISO, onder meer voor het aanmelden van nieuwe of gewijzigde processen waarin persoonsgegevens worden verwerkt en de behandeling van verzoeken van burgers voor de uitoefening van privacyrechten. De contactpersoon privacy wordt tevens geacht met onder meer de FG, PO en CISO een netwerk te vormen om de aanwezigheid van kennis over informatiebeveiliging en privacy uit te wisselen en de naleving van de AVG en de Wpg in de organisatie te borgen. Uitgangspunt van zowel informatiebeveiligings-beleid als privacybeleid hierbij is de contactpersonen in de afdelingen zoveel mogelijk te laten optreden als contactpersonen voor zowel informatiebeveiliging als privacy (security en privacy specialisten binnen de afdelingen).

Belangrijke verantwoordelijkheden van de contactpersoon privacy:
• Binnen de afdeling adviseren over de naleving van de AVG en de Wpg;
• Het in behandeling nemen van verzoeken voor de uitoefening van privacyrechten (bijvoorbeeld verzoek om inzage, correctie of verwijdering) ten aanzien van persoonsgegevens die door de afdeling worden verwerkt;
• Nieuwe verwerkingen of wijzigingen in bestaande verwerkingen van persoonsgegevens namens de afdelingsmanager aanmelden bij de FG/PO voor toetsing aan beleid en opname in het register van verwerkingen;
• Jaarlijks de verwerkingen van de afdeling in het register van verwerkingen controleren op volledigheid en actualiteit;
• Deelnemen in het netwerk voor privacy en informatiebeveiliging van de organisatie.

In de basis betreft het zijn van contactpersoon privacy een coördinerende rol die naar verwachting 12 tot 24 uur inzet per jaar vergt, mede afhankelijk van het aantal en soort verwerkingen binnen de afdeling.

3.2 Governance

De governance rond privacy wordt conform de Sturingsfilosofie 2022 uitgevoerd volgens het three lines-model.[7] In onderstaande figuur is dit weergegeven:

3de lijn	FG & CISO	Deze lijn gaat over kaders stellen, onafhankelijk toezicht, strategisch advies, toetsen en rapporteren.
2de lijn	PO, medewerkers Informatie-beveiliging van I&P, Kwaliteitsmedewerkers afdelingen	Deze lijn gaat over adviseren en ondersteunen van proceseigenaren om processen en systemen te verbeteren.
1e lijn	Proceseigenaar (management) en medewerkers	Deze lijn is feitelijk verantwoordelijk voor het functioneren van de werkprocessen. Hier moet kennis en kunde worden geborgd. De contactpersonen privacy spelen hierbij een belangrijke rol.

7) https://www.iia.nl/kenniscentrum/vaktechnische-publicaties/three-lines-model-updated---nl

Forum IB & Privacy
Uitgangspunt is dat elke twee maanden een overleg wordt georganiseerd door CISO en FG met medewerkers uit de eerste en tweede lijn (met name de contactpersonen IB&P) om ontwikkelingen op het gebied van informatiebeveiliging en privacy te bespreken en informatie op te halen uit de organisatie.

Portefeuillehoudersoverleg en overleg gemeentesecretaris IB & Privacy
Uitgangspunt is dat er één keer per maand overleg met de gemeentesecretaris en de concerncontroller is en één keer per kwartaal met de portefeuillehouder uit het college waarbij CISO en FG relevante ontwikkelingen op het gebied van informatiebeveiliging en privacy bespreken.

Overleg specialisten IB & Privacy
De CISO, FG en PO werken dagelijks samen en bespreken doorlopend de actuele ontwikkelingen op het gebied van informatiebeveiliging en privacy.

Rapportage
Bij de begroting en jaarrekening worden speerpunten toegelicht en indien nodig financiële middelen gevraagd voor informatiebeveiliging en privacy. De FG doet daarnaast jaarlijks formeel verslag over privacy in de organisatie middels een jaarrapportage gegevensbescherming. Voor het toezicht wordt door de FG gebruik gemaakt van het borgingsproduct van de VNG als beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente.

3.3 Beleidsuitwerking

De kaders in dit privacybeleid vormen de uitgangspunten voor de ontwikkeling van nadere beleidsdocumenten en instructies om verder richting te geven aan de dagelijkse praktijk.

Het gaat om bijvoorbeeld:
- De privacyverklaring van de gemeente Bergen op Zoom op de website;
- Een handreiking informatiebeveiliging en privacy met afspraken voor veilig (thuis)werken;
- Een procedure voor het melden en behandelen van datalekken;
- Een procedure voor de uitoefening van de rechten van betrokkenen;
- Een procedure en formats voor privacyovereenkomsten, zoals verwerkersovereenkomsten;
- Een procedure en formats voor de uitvoering van DPIA's.

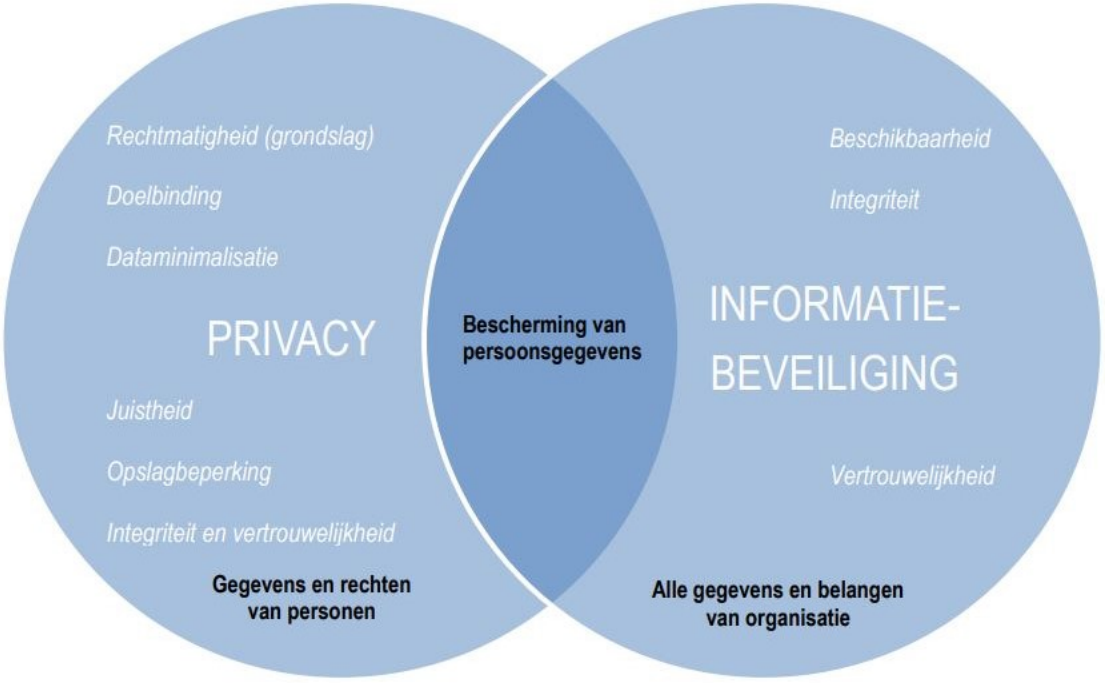
Daarnaast kan meer domein-, afdeling of processpecifiek of door nieuwe wetgeving een nadere uitwerking van privacybeleid benodigd zijn. Bijvoorbeeld op het gebied van het sociaal domein, veiligheid en handhaving, publieksdiensten of personeelszaken. Dergelijke gerichte uitwerkingen worden door de betreffende afdelingen opgesteld. De uitwerkingen worden altijd aan de CISO, FG en PO voorgelegd voor advies en toetsing aan wet en beleid.

Het privacybeleid en de nadere taak- en domeinspecifieke uitwerkingen daarvan worden overzichtelijk aan de medewerkers gepresenteerd via een communicatiesite privacy als onderdeel van het intranet van de gemeente (BoZnet).

4. Informatiebeveiliging

Naast dit privacybeleid is er informatiebeveiligingsbeleid vastgesteld door het college (IB-Beleid 2021-2024, vastgesteld in 2021). Hierin wordt beschreven welke uitgangspunten gelden op het gebied van informatiebeveiliging in de organisatie. Het informatiebeveiligingsbeleid is gebaseerd op de voor de gemeente geldende beveiligingsnormen zoals vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO). De BIO is sinds 1 januari 2020 van kracht en is er op gericht steeds de belangrijkste kwaliteitskenmerken van informatie te waarborgen, te weten: de beschikbaarheid, de integriteit en de vertrouwelijkheid van informatie. Hiervoor moeten in de organisatie verschillende technische en organisatorische maatregelen worden getroffen. Denk aan het inregelen van autorisaties om onbevoegde toegang te voorkomen en het hebben van een betrouwbare back-up om verlies van informatie te voorkomen. Maar bijvoorbeeld ook een goede firewall om de gemeente te beschermen tegen hackers. Daarbij wordt door de gemeente op basis van risicoanalyses periodiek beoordeeld welke beveiligingsmaatregelen moeten worden getroffen of aangescherpt.

De AVG en Wpg vereisen ook dat persoonsgegevens veilig worden verwerkt en hiervoor passende technische en organisatorische maatregelen worden getroffen.[8] Daarmee zijn informatiebeveiliging en privacy onlosmakelijk met elkaar verbonden. Informatiebeveiliging is immers een randvoorwaarde om privacy te borgen.
De samenhang tussen informatiebeveiliging en privacy is weergegeven in onderstaande afbeelding.



Wat per proces een passend beschermingsniveau is wordt mede bepaald door het soort persoonsgegeven dat wordt verwerkt (bijvoorbeeld gevoelig of bijzonder), de beschikbaarheid en toepasbaarheid van de beveiligingsmaatregelen en de kosten die verbonden zijn aan de maatregel in relatie tot het risico en de gevolgen van een onrechtmatige verwerking van de persoonsgegevens. Voor het verwerken van persoonsgegevens in het kader van de Wpg worden daarnaast specifieke eisen gesteld aan informatiebeveiliging.[9]

5. Instrumenten

Het waarborgen van privacy (AVG en Wpg) en informatiebeveiliging (BIO) is een doorlopend proces. In dit hoofdstuk worden de instrumenten besproken die voor het waarborgen van privacy worden ingezet.

5.1 Bewustwording

De toegenomen afhankelijkheid van internet in het zakelijk verkeer, de voortschrijdende digitalisering van de dienstverlening, het toegenomen gebruik van sociale netwerken en de opslag van informatie in de cloud creëren beveiligingsrisico's voor persoonsgegevens. De gemeente ziet in dat de mens hierbij een belangrijke schakel vormt en dat de mate waarin medewerkers bewust zijn van de risico's en veilig gedrag vertonen de sterkte en zwakte van deze schakel bepaalt. De meeste datalekken worden ook veroorzaakt door onbewust verkeerd handelen. Om het risico op onbewust verkeerd handelen te bestrijden en in het algemeen een zorgvuldige omgang met persoonsgegevens te waarborgen geeft de gemeente structureel aandacht aan het verhogen van het beveiligingsbewustzijn van medewerkers. Bewust worden en blijven wordt gerealiseerd door een introductiebijeenkomst informatiebeveiliging

8) Artikel 5 lid 1 onder f en 32 AVG en artikel 4a Wpg.
9) Artikel 4a Wpg in samenhang met artikel 6:1a Besluit politiegegevens.

en privacy te verzorgen voor nieuwe medewerkers en jaarlijks een training (e-learning of andere activiteit of evenement) aan te bieden voor alle medewerkers en/of specifieke doelgroepen. Daarnaast wordt voortdurend gewerkt aan het vergroten van kennis en bewustzijn door het actueel houden van beleid en procedures, voorlichting door experts zoals de CISO, FG en PO en de publicatie van artikelen en nieuws middels hiervoor intern ingerichte digtale communicatiekanalen. Op deze manier worden managers en medewerkers in staat gesteld te handelen in overeenstemming met de toepasselijke regelgeving en in het algemeen verantwoordelijkheid te nemen voor een zorgvuldige omgang met persoonsgegevens.

5.2 Register van verwerkingen

De gemeente is verantwoordelijk voor het bijhouden van een register van alle werkprocessen waarbij persoonsgegevens worden verwerkt.[10] Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:
- De naam en contactgegevens van de gemeente als verwerkingsverantwoordelijke en van de FG;
- De doelen en de grondslag van de verwerking;
- Een beschrijving van de soort persoonsgegevens (categorieën van persoonsgegevens) en de daarbij horende betrokkenen (categorieën van betrokkenen);
- Een beschrijving van met wie de persoonsgegevens worden gedeeld (ontvangers);
- De bewaartermijnen van de persoonsgegevens;
- Een algemene beschrijving van de beveiligingsmaatregelen.

De gemeente zorgt voor een actueel en volledig register van verwerkingen. De FG speelt een leidende rol bij het opzetten en bewaken van de daarvoor benodigde structuur. De afdelingen zijn verantwoordelijk voor het bijhouden van het register en het melden van nieuwe verwerkingen of wijzigingen in bestaande verwerkingen bij de FG en/of PO voordat met deze verwerkingen wordt begonnen. De FG of PO registreert wijzigingen in het register. Met het register kan de gemeente laten zien hoe aan de AVG en Wpg wordt voldaan. Op verzoek van de AP dient het register overhandigd te kunnen worden ter controle.

5.3 Procedure datalekken

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan of als onrechtmatige verwerking van persoonsgegevens niet uitgesloten kan worden.[11] Bijvoorbeeld bij verlies of diefstal van apparaten of documenten, het verkeerd adresseren van een brief of e-mail, toegang zonder autorisatie of inbraak door een hacker. De gemeente is verplicht om een datalek te melden bij de Autoriteit Persoonsgegevens (AP) als het datalek “een risico” inhoudt voor de personen van wie de gegevens zijn gelekt. De getroffen personen moeten ook door de gemeente worden geïnformeerd als het datalek voor hen een “hoog risico” inhoudt. De melding bij de AP moet binnen 72 uur na ontdekking plaatsvinden. Het niet melden van een datalek vormt een overtreding van de AVG of de Wpg. De AP kan voor een overtreding van de AVG of de Wpg zoals het niet of te laat melden van een datalek een boete opleggen. Elke medewerker van de gemeente moet dan ook alert zijn op een datalek en is verplicht elk datalek of vermoeden ervan direct intern te melden volgens een daarvoor vastgestelde procedure. Voor de meldingsprocedure is een aparte webpagina ingericht en toegankelijk gemaakt via het hoofdmenu op intranet (BoZnet). De melding wordt zo snel mogelijk besproken in een datalekteam (in de basis: CISO, FG, PO en concernjurist). Het datalekteam adviseert de verantwoordelijk afdelingsmanager over de te treffen maatregelen en het melden van het datalek bij de AP en de getroffen personen. De afdelingsmanager is verantwoordelijk voor de uitvoering van de maatregelen en de melding bij de AP en betrokkenen. De gemeente houdt verder een register bij van alle incidenten met persoonsgegevens. Het register wordt periodiek geëvalueerd om op basis van de hierdoor verkregen inzichten maatregelen te treffen en te controleren om herhaling van datalekken te voorkomen en de kans op nieuwe te verkleinen.

5.4 Risicobeheersing

De gemeente neemt verder onderstaande maatregelen om risico’s bij de verwerking van persoonsgegevens in kaart te brengen en zo veel mogelijk te verminderen.

5.4.1 DPIA

10) Artikel 30 AVG en artikel 31d Wpg.
11) Artikel 33 en 34 AVG en artikel 33a Wpg.

Privacy begint aan de voorkant. Voorafgaand aan risicovolle verwerkingen van persoonsgegevens voert de gemeente dan ook een privacyrisicoanalyse uit, ook wel een DPIA genoemd. Op basis van een DPIA wordt nagegaan of bij een verwerking van persoonsgegevens de privacy van betrokkenen geborgd is. Het uitvoeren van een DPIA is op grond van de AVG en de Wpg verplicht als een verwerking een hoog privacyrisico oplevert voor betrokkenen.[12] Een hoog risico wordt bijvoorbeeld aangenomen bij grootschalige verwerkingen of bij verwerkingen van gevoelige persoonsgegevens. Met een DPIA wordt dan inzicht verkregen in de risico's van de verwerking en welke maatregelen kunnen worden toegepast om de risico's te beperken. De afdelingsmanager is als proceseigenaar verantwoordelijk voor het uitvoeren van een DPIA. Bij het uitvoeren van de DPIA wordt de FG om advies gevraagd. Een DPIA moet worden uitgevoerd voordat met de verwerking van de persoonsgegevens wordt gestart. De uitkomsten van de DPIA moeten namelijk gemotiveerd worden betrokken bij de beslissing om de verwerking van de persoonsgegevens al dan niet te starten.

Om te bepalen of het uitvoeren van een volledige DPIA noodzakelijk is wordt gebruik gemaakt van de laatste versie van de Pre-scan DPIA van het Centrum Informatiebeveiliging en Privacybescherming (CIP) of de Pre-DPIA in de integrale risico- en privacy-analyse (IRPA-)tool van de Informatiebeveiligingsdienst (IBD). Als de uitkomst hiervan is dat de beoogde verwerking resulteert in een hoog privacy risico voor de betrokkenen, wordt een volledige DPIA uitgevoerd. Een volledige DPIA wordt uitgevoerd met het Model DPIA Rijksdienst of de DPIA in de IRPA-tool van de IBD. De PO ondersteunt de proceseigenaar bij de uitvoering van een DPIA. Nadere instructies en actuele versies van genoemde modellen en tools worden door de FG en PO beschikbaar gesteld, in de regel via de communicatiesite privacy als onderdeel van het intranet van de gemeente (BoZnet).

5.4.2 Privacy by design en by default

Bij het verwerken van persoonsgegevens zijn op grond van de AVG en de Wpg de beginselen van gegevensbescherming door ontwerp (privacy by design) en gegevensbescherming door standaardinstellingen (privacy by default) van toepassing.[13]

Privacy by design houdt in dat de gemeente al bij het ontwerpen of inrichten van een nieuw systeem of proces ervoor zorgt dat persoonsgegevens goed worden beschermd en betrokkenen hun rechten goed kunnen uitoefenen. Bijvoorbeeld door onder andere de toegangsbeveiliging tot de persoonsgegevens goed te regelen en ervoor te zorgen dat persoonsgegevens wanneer nodig (automatisch) worden versleuteld of verwijderd. Door het borgen van privacyaspecten aan het begin van een proces wordt ervoor gezorgd dat risico's zo veel mogelijk worden beperkt.

Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen neemt om ervoor te zorgen dat, als standaard, alléén die persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel. Dus dat de standaardinstellingen van een programma, app, website, dienst of apparaat zodanig zijn ingesteld dat steeds maximale privacy wordt nagestreefd. Bijvoorbeeld door bij de aanmelding voor een nieuwsbrief niet meer gegevens te vragen dan nodig of bij een app niet de locatie van gebruikers te laten registreren als dat niet nodig is (dataminimalisatie).

Privacy by design en privacy by default worden bij de aanbesteding en/of aanschaf van nieuwe systemen en/of diensten steeds in aanmerking genomen. Bijvoorbeeld door privacy eisen bij inkoop standaard op te nemen in het Programma van Eisen. De specifieke inhoudelijke eisen dienen daarbij steeds door de verantwoordelijke vakafdeling te worden gesteld.

5.4.3 Verwerkers- en andere privacyovereenkomsten

Wanneer de gemeente bij de uitvoering van haar taken samenwerkt met andere organisaties en daarbij persoonsgegevens worden verwerkt, worden door de gemeente steeds schriftelijke afspraken gemaakt over de beveiliging van de persoonsgegevens, de behandeling van datalekken en de rechten van betrokkenen.

Wanneer de gemeente een andere organisatie inschakelt om voor de gemeente persoonsgegevens te verwerken, wordt deze andere organisatie in de regel beschouwd als een verwerker voor de gemeente. Bijvoorbeeld een leverancier van software, netwerkdiensten of dataopslag. De gemeente schakelt alleen verwerkers in die voldoende garanties kunnen bieden om de verwerking van persoonsgegevens te laten voldoen aan de eisen uit de AVG en/of de Wpg. De afspraken met een verwerker worden schriftelijk vastgelegd in een zogenaamde verwerkersovereenkomst voordat de dienstverlening aanvangt. De ge-

12) Artikel 35 AVG en artikel 4c Wpg.
13) Artikel 25 AVG en artikel 4a en 4b Wpg.

meente maakt hierbij verplicht gebruik van de meest recente versie van de standaard verwerkersovereenkomst voor gemeenten van de IBD. De eisen die in dit model worden gesteld worden al in aanmerking genomen bij de aanbesteding van nieuwe systemen en/of diensten.

Verder werkt de gemeente ook samen met organisaties die geen verwerker voor de gemeente zijn maar waarmee wel persoonsgegevens worden uitgewisseld. Bijvoorbeeld met zorgaanbieders of in samenwerkingsverbanden op het gebied van zorg en veiligheid. Ook dan maakt de gemeente schriftelijke afspraken met die andere organisaties. Er wordt dan bijvoorbeeld een gegevensuitwisselingsovereenkomst of privacy-convenant afgesloten.

Actuele versies van modelovereenkomsten worden beschikbaar gesteld door de FG en PO, in de regel via de communicatiesite privacy als onderdeel van het intranet van de gemeente (BoZnet). De afdelingsmanager is als proceseigenaar verantwoordelijk voor het afsluiten van de benodigde privacyovereenkomst. De betrokken afdeling controleert voorts periodiek de naleving van de gemaakte afspraken om de veilige verwerking van persoonsgegevens te borgen en hierbij regie te behouden.

5.4.4 Privacy audits Wpg

In het kader van de Wpg bestaat een verplichting om met ingang 2021 elke 4 jaar een externe privacy audit te laten uitvoeren naar de naleving van de Wpg en hierover aan de AP te rapporteren.[14] Daarnaast dient er op dit gebied ieder jaar een interne audit te worden uitgevoerd. Aan de hand hiervan kan steeds worden vastgesteld of de gemeente bij de verwerkingen onder de Wpg voldoet aan de wettelijke eisen en kan waar nodig worden bijgestuurd. De afdelingsmanagers van de organisatieonderdelen waar de boa's werkzaam zijn, zijn verantwoordelijk voor de uitvoering van de audits.

6. Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt.[15] Ook de Wpg regelt dat.[16] Deze rechten worden ook wel de rechten van betrokkenen genoemd.

6.1 Informatieplicht

Wanneer een verwerking van persoonsgegevens plaatsvindt, moet voor betrokkenen duidelijk zijn dat dit zo is en wat het doel van de verwerking is. In het algemeen worden betrokkenen hierover door de gemeente geïnformeerd via de privacyverklaring op de website van de gemeente. Meer specifiek moet per verwerking deze informatie beschikbaar zijn op het moment dat er een verwerking gaat plaatsvinden en/of klantcontact is, onafhankelijk of dit in persoon is of digitaal. Deze informatie kan bijvoorbeeld via een aanvraagformulier, brief of folder of mondeling worden verstrekt. Elke afdeling heeft hierin een eigen verantwoordelijkheid. De betrokkene wordt niet nogmaals geïnformeerd als hij of zij al weet dat de gemeente persoonsgegevens van hem of haar verwerkt, en weet waarom en voor welk doel dat gebeurt.

6.2 Rechten van betrokkenen

Op grond van de AVG en de Wpg heeft iedereen verder de volgende rechten om controle en invloed uit te oefenen over zijn of haar persoonsgegevens:

- Recht op inzage: Betrokkenen hebben de mogelijkheid om de persoonsgegevens die van hun worden verwerkt in te zien en hiervan een kopie te krijgen. De betrokkene hoeft hiervoor geen reden op te geven maar hij mag niet onredelijk grote of overdreven veel verzoeken in korte tijd indienen.
- Recht op rectificatie (correctie van gegevens): Als duidelijk is dat de gegevens niet kloppen, kunnen betrokkenen een verzoek indienen bij de gemeente om gegevens te corrigeren.
- Recht om vergeten te worden (wissen van gegevens): Behoudens wettelijke beperkingen hebben betrokkenen het recht om persoonsgegevens te laten wissen, bijvoorbeeld wanneer de toestemming

14) Artikel 33 Wpg.
15) Artikel 13 t/m 20 AVG.
16) Artikel 24 t/m 28 Wpg.

hiervoor is ingetrokken en er geen andere rechtsgrond bestaat voor de verwerking. Op gegevens die worden verwerkt voor de uitvoering van een publieke taak is dit recht niet van toepassing.
• Recht op beperking van de verwerking. Betrokkenen kunnen vragen om beperking van een verwerking, bijvoorbeeld om bepaalde gegevens tijdelijk niet te gebruiken of af te schermen als gegevens mogelijk onjuist zijn of mogelijk onrechtmatig worden verwerkt.
• Recht op dataportibaliteit (overdraagbaarheid van gegevens). Betrokkenen kunnen vragen om hun persoonsgegevens te ontvangen of door te sturen, bijvoorbeeld bij een verhuizing. Dit recht geldt alleen voor verwerkingen onder de AVG (niet onder de Wpg) en is niet van toepassing op gegevens die worden verwerkt voor de uitvoering van een publieke taak.
• Recht op bezwaar: Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens. De gemeente moet aan bezwaren tegemoetkomen, tenzij er gerechtvaardigde gronden zijn voor de verwerking en/of de wet voorschrijft dat de gemeente de gegevens verwerkt. Dit recht geldt alleen voor verwerkingen onder de AVG (niet onder de Wpg).
• Recht niet te worden onderworpen aan geautomatiseerde besluitvorming, waaronder profilering. Betrokkenen hebben recht op een menselijke blik bij besluiten.

In een aparte handreiking worden de verschillende rechten nader toegelicht en wordt aangegeven hoe de gemeente hiermee omgaat. Die handreiking is voor alle medewerkers beschikbaar via de communicatiesite privacy als onderdeel van het intranet van de gemeente (BoZnet).

6.3 Indienen verzoek of klacht

Om gebruik te maken van de hiervoor genoemde rechten kunnen betrokkenen een verzoek indienen bij de gemeente. Dit verzoek kan zowel schriftelijk als elektronisch (via e-mail of formulier op de gemeentelijke website) ingediend worden. De gemeente heeft één maand de tijd om het verzoek te beoordelen. Deze termijn kan bij complexe verzoeken met twee maanden worden verlengd. De gemeente moet altijd binnen de wettelijke termijn laten weten wat er met het verzoek gaat gebeuren. De beslissing op een verzoek geldt als een besluit in de zin van de Algemene wet bestuursrecht. Als het verzoek niet wordt opgevolgd is er dan ook de mogelijkheid hiertegen bezwaar en beroep in te stellen. Als betrokkene vermoedt dat persoonsgegevens worden verwerkt in strijd met de wet kan ook een klacht worden ingediend bij de Autoriteit Persoonsgegevens (AP).

7. Inwerkingtreding, evaluatie en herziening

Dit privacybeleid treedt in werking na vaststelling door het college van burgemeester en wethouders en vervangt het privacybeleid zoals dat door het college is vastgesteld op 3 juli 2018. De organisatie zal steeds kijken of het beleid nog voldoet of zo nodig aangepast moet worden. Technologische, juridische en maatschappelijke ontwikkelingen op het gebied van privacy volgen elkaar immers snel op. In de regel wordt het privacybeleid in ieder geval elke vier jaar herzien. Indien zich eerder grote wijzigingen voordoen vindt actualisatie eerder plaats. De actuele versie van het privacybeleid is steeds te vinden op de website en het intranet van de gemeente.

Het college van Burgemeester en Wethouders van Bergen op Zoom,

In zijn vergadering van 30 mei 2023,

B E S L U I T:

het Algemeen Privacybeleid vast te stellen.

secretaris,

Dhr. mr. drs. ing. M. van Vliet

burgemeester,

Dhr. dr. F.A. Petter

Bijlage 1 Taken en verantwoordelijkheden gegevensbescherming

1	**Register van verwerkingen** - De proceseigenaar is verantwoordelijk voor de actualiteit van de verwerkingen in het register van zijn afdeling. - De FG en de PO zijn verantwoordelijk voor het beheer en de coördinatie van de actualisatie van het register van verwerkingen.				
		Proceseige-naar	**CISO**	**FG**	**PO**
	Actief melden van nieuwe of gewijzigde verwerkingen bij de PO en de FG	X			
	Zorgdragen voor actualiteit van verwerkingen	X			
	Coördinatie van de actualisatie van het register van verwerkingen			X	X
	Beheer van het register van verwerkingen			X	X
	Toetsing op kwaliteit, actualiteit, juistheid en volledigheid van het register van verwerkingen			X	

2	**Privacy overeenkomsten** - De proceseigenaar is verantwoordelijk voor het afsluiten, beheren en actualiseren van verwerkers- en andere privacyovereenkomsten. - De FG en PO zijn verantwoordelijk voor de beschikbaarheid van actuele modellen voor verwerkers- en andere privacyovereenkomsten. - De PO geeft inhoudelijk advies en ondersteuning aan de proceseigenaar over het afsluiten van verwerkers- en andere privacyovereenkomsten. - De CISO geeft inhoudelijk advies aan de proceseigenaar over voorwaarden en onderdelen in verwerkers- of andere privacyovereenkomsten rondom informatiebeveiliging. - De FG adviseert over en ziet toe op het invullen van de verantwoordelijkheden van de proceseigenaar en de PO. De FG ziet daarbij toe op een handelwijze volgens de privacywetgevingen op de integriteit, vertrouwelijkheid en beschikbaarheid van de centrale registratie.				
		Proceseigenaar	**CISO**	**FG**	**PO**
	Afsluiten van verwerkers- en andere privacyovereenkomsten	X			
	Actualiseren en beheren van de modelovereekomsten.			X	X
	Verplicht advies ten aanzien van de samenwerking met derden en verwerkers- of andere privacyovereenkomsten.		X	X	X
	Decentrale archivering van verwerkers-overeenkomsten	X			
	Toezicht op de registratie en uitvoering van verwerkers- en andere privacyovereenkomsten.			X	

3	**Overleg Informatiebeveiliging en privacy** - De CISO en FG organiseren en zitten een gemeentebreed informatiebeveiligings- en privacyoverleg voor. - De CISO, FG en PO nemen deel aan organisatiebrede en onderdeelspecifieke overleggen die informatiebeveiligings- en privacyvraagstukken behandelen.

	- De CISO, FG en PO nemen op uitnodiging deel aan team-, project- en themaoverleggen, indien hierbij informatiebeveiligings- of privacyvraagstukken aan de orde zijn. - De proceseigenaar wijst een contactpersoon informatieveiligheid & privacy aan binnen de afdeling.

		Proceseigenaar	CISO	FG	PO
	Voorzitten informatiebeveiligings- en privacy overleg		X	X	
	Deelnemen aan informatiebeveiligings- en privacyoverleg		X	X	X
	Project-, team- en thema-overleggen m.b.t informatiebeveiligings- en privacyvraagstukken bijwonen		X	X	X
	Aanwijzen decentraal contactpersoon Informatiebeveiliging en privacy	X			

4	**Datalekken** - De proceseigenaar is verantwoordelijk voor het intern melden en afhandelen van datalekken binnen de afdeling, het inventariseren van feiten en omstandigheden, de eventuele externe melding bij de toezichthouder en betrokkenen en eventuele externe communicatie rond het incident. - De proceseigenaar is tevens verantwoordelijk voor de implementatie van adviezen die voortkomen uit onderzoek en/of zijn opgenomen in de rapportage van het datalekteam. - De PO is verantwoordelijk voor inhoudelijke advisering en ondersteuning van de proceseigenaar bij het doorlopen van de procedure. - De FG en de CISO staan zowel de proceseigenaar als de PO bij in raad en daad bij het doorlopen van de procedure. - De CISO, FG en PO zijn verantwoordelijk voor de registratie van het incident en de toetsing op implementatie van de adviezen uit de rapportages.

		Proceseigenaar	CISO	FG	PO
	Intern melden van een datalek	X			
	Inventariseren van feiten en omstandigheden	X	X		X
	Uitvoeren analyse, opstellen verslag en verstrekken van intern advies		X	X	X
	In geval van dilemma's in analyse en/of advies of grote risico's afstemming verzorgen met directie en bestuur	X	X	X	
	Melding bij toezichthouder en betrokkenen en eventuele externe communicatie	X			
	Implementeren adviezen	X			
	Registratie incident		X	X	X
	Toetsing op implementatie adviezen		X	X	X

5	**Advies en voorlichting** - De CISO, FG en PO geven gevraagd en ongevraagd advies aan de organisatie (medewerkers en management) en bestuur met betrekking tot privacyvraagstukken. - De proceseigenaar is verantwoordelijk voor aandacht voor informatieveiligheid en privacy op de afdeling.

		Proceseigenaar	CISO	FG	PO
			X	X	X

	Voorlichting en communicatie over informatiebeveiliging en privacy (bewustwording) aan de organisatie		X	X	X
	Continue aandacht voor informatieveiligheid en privacy op de afdeling	X			

6	**DPIA** - De proceseigenaar is verantwoordelijk voor het uitvoeren van DPIA's en het effectueren van de maatregelen naar aanleiding van een DPIA. - De PO is verantwoordelijk voor inhoudelijke advisering en ondersteuning van de proceseigenaar bij het doorlopen van de procedure. - De CISO is verantwoordelijk voor inhoudelijke advisering en ondersteuning van de proceseigenaar voor het onderdeel informatiebeveiliging. - De FG staat zowel de proceseigenaar als de PO bij in raad en daad bij het doorlopen van de DPIA procedure en het geeft inhoudelijk en aan het eind formeel verplicht advies.				
		Proceseigenaar	**CISO**	**FG**	**PO**
	Uitvoeren van een DPIA	X			X
	Inhoudelijk advies en ondersteuning bij doorlopen van de DPIA procedure		X		X
	Opstellen DPIA-verslag, inclusief aanbevelingen FG, en zorgdragen voor nadere besluitvorming en registratie	X			X
	Implementeren maatregelen voortkomend uit DPIA	X			
	Toetsen op de procedure, de resultaten, de effectuering en de naleving van de maatregelen uit de DPIA			X	

7	**Klachten** - De proceseigenaar is verantwoordelijk voor de behandeling van klachten met betrekking tot de verwerking en bescherming van persoonsgegevens. Dit eventueel in samenwerking met de gemeentelijke klachtbehandelaar en/of FG. - De PO en de CISO zijn verantwoordelijk voor de inbreng van inhoudelijke en procedurele kennis op het gebied van informatiebeveiliging en privacy die eventueel nodig is voor het doorlopen van de klachtafhandelingsprocedure. - De FG ziet toe op de kwaliteit en de correcte afhandeling van de klacht.				
		Proceseigenaar	**CISO**	**FG**	**PO**
	Het behandelen van klachten	X			
	Inbreng van inhoudelijke en procedurele kennis informatiebeveiliging en privacy		X		X
	Toezien op kwaliteit en correcte afhandeling van klacht			X	

8	**Rechten van betrokkenen** - De proceseigenaar is verantwoordelijk voor de afhandeling van verzoeken van de rechten van betrokkenen met betrekking tot de persoonsgegevens die onder zijn verantwoordelijkheid vallen. - De PO coördineert de afdelingsoverstijgende verzoeken van betrokkenen. Dit betekent dat deze de verzoeken in ontvangst neemt, het verzoek uitzet binnen de organisatie, informatie verzamelt en een terugkoppeling geeft aan de betrokkene. - De FG ziet toe op de afhandeling van de verzoeken van betrokkenen.

		Proceseigenaar	CISO	FG	PO
	Het in behandeling nemen van verzoeken	X			
	Ontvangst en coördinatie, inclusief terugkoppeling aan verzoeker bij afdelingsoverstijgende verzoeken				X
	Inhoudelijk adviseren en ondersteunen proceseigenaar bij behandeling verzoek				X
	Toezicht op procedure en kwaliteit			X	
	De behandeling van bezwaar en beroep tegen een beslissing op een verzoek	X			X

9	**Ontwikkeling en beheer beleid** - De CISO, FG en PO zijn verantwoordelijk voor de ontwikkeling, het beheer, de optimalisatie en de interne communicatie rond algemeen informatiebeveiligings- en privacybeleid. - De proceseigenaar is verantwoordelijk voor de uitvoering van het beleid ten aanzien van de persoonsgegevens die onder zijn verantwoordelijkheid vallen. - De FG is verantwoordelijk voor de toetsing op de uitvoer van het beleid.				
		Proceseigenaar	**CISO**	**FG**	**PO**
	De ontwikkeling, het beheer, de optimalisatie en de interne communicatie rond algemeen informatiebeveiligings- en privacybeleid		X	X	X
	Ten uitvoer brengen van het beleid	X			
	Toezicht op de uitvoering van het beleid			X	