gemeente Brunssum

GEMEENTEBLAD

Officiële uitgave van de gemeente Brunssum

Nr. 39317

20 februari 2019

Beleidsregel van het college van burgemeester en wethouders van de gemeente Brunssum houdende regels omtrent privacy Privacybeleid gemeente Brunssum

Het college van B&W heeft op 12 februari 2019 het 'Privacybeleid gemeente Brunssum' vastgesteld. Dit beleid treedt de dag na bekendmaking in werking.

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. De AVG bepaalt dat de gemeente een privacybeleid moet opstellen. Het 'Privacybeleid gemeente Brunssum' is dan ook in lijn met de AVG en andere relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Iedereen heeft recht op privacy. Ook de gemeente Brunssum verzamelt en gebruikt veel persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van de taken die een gemeente heeft. De gemeente is dan ook verantwoordelijk voor de bescherming van deze persoonsgegevens. Doel van het privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente persoonsgegevens verwerkt.

1 INLEIDING

1.1 Algemene toelichting

Binnen de gemeente Brunssum wordt veel gewerkt met persoonsgegevens van burgers en medewerkers. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van wettelijke gemeentelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat.
In deze tijd gaat ook de gemeente mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van (persoons)gegevens. De gemeente is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, informatiemanagement, dataminimalisatie, transparantie, gebruikerscontrole en opleidingen en creëren van bewustwording voor medewerkers.
Het bestuur, management en medewerkers spelen een cruciale rol bij het waarborgen van privacy. De gemeente Brunssum geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacybeleid van gemeente Brunssum is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

1.2 Toelichting Privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden.
Persoonsgegevens zijn hierbij: 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd'.
Onder verwerking wordt verstaan: 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geheel of gedeeltelijke geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens'.

1.3 Toelichting Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.

Deze aspecten zijn:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de bedrijfsvoering van de organisatie. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.4 Vervlechting Privacy, Informatiebeveiliging en Informatiemanagement

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel van privacy is. Informatiebeveiliging is noodzakelijk bij het zorgvuldig omgaan met (persoons)gegevens. Beide begrippen staan naast elkaar en zijn van elkaar afhankelijk.

Een ander belangrijk aspect bij privacy en informatiebeveiliging is informatiemanagement. Het betreft de wijze waarop een organisatie met informatie omgaat. De doelstelling van informatiemanagement is het zorgdragen voor de beschikbaarheid van de gevraagde informatie, zodat de organisatie de geplande resultaten kan leveren.
Vraagstukken over gegevensbronnen, locatie, gegevenstypen, vertrouwelijkheid, risico classificatie, bewaartermijnen, etc. worden veelal bepaald in het informatiemanagement proces. Goed informatiemanagement is dus noodzakelijk voor privacybescherming en informatiebeveiliging.

2 DOEL EN REIKWIJDTE

2.1 Ambitie

De gemeente Brunssum wil bijdragen aan een betrouwbare overheid. Betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met hun gegevens omgaat. Door alle ontwikkelingen rondom gegevensverwerking wordt dit steeds complexer. Door nieuwe wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens is het overtreden hiervan een serieus risico. Informatiebeveiliging en bescherming van persoonsgegevens is altijd een kosten-baten afweging, waarbij 100% veiligheid een utopie is. In elk proces en in elke ketensamenwerking zit wel een zwakke schakel. De gemeente streeft een adequaat niveau van privacybescherming en informatiebeveiliging na waarbij voor het reduceren van risico's, voortdurend afwegingen worden gemaakt om de juiste balans te vinden tussen wetgeving, de taakstelling van de organisatie en de persoonlijke levenssfeer van betrokkenen.

De gemeente heeft de ambitie om op rechtmatige, veilige en transparante wijze, gegevens van burgers, medewerkers en organisaties ten behoeve van administraties en diensten te verwerken.

Dit wordt ondersteund door de privacymissie van de gemeente Brunssum :

De gemeente Brunssum hecht veel waarde aan de privacy en beveiliging van gegevens van haar burgers, medewerkers en organisaties bij de verwerking van deze gegevens. De verwerking van persoonsgegevens is in control en transparant teneinde de kwaliteit en veiligheid van deze gegevens op een betrouwbare manier te waarborgen. De gemeente gaat hierbij klantgericht, professioneel en integer te werk.

2.2 Doel

Doel van dit privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen dat de gemeente Brunssum de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de geldende wet- en regelgeving.

Het privacybeleid draagt bij aan:
- Het beschermen van de privacy van personen van wie de gemeente gegevens verwerkt of laat verwerken,
- Maatschappelijk vertrouwen en draagvlak,
- Het beheersen van gemeentelijke afbreuk- en aansprakelijkheidsrisico's,
- Het met vertrouwen verantwoording kunnen afleggen aan de burger, het College van B&W, de raad, medewerkers, waar nodig de Autoriteit Persoonsgegevens of de rechter,
- Het in kunnen spelen op wettelijke en technologische ontwikkelingen.

2.3 Doelgroep

Doelgroep	Relevantie beleid
College van B&W	Eindverantwoordelijk voor het waarborgen van de privacy van burgers en medewerkers. Vaststellen van het privacybeleid.
Gemeentesecretaris / Algemeen Directeur	Verantwoordelijk voor kaderstelling en sturing met betrekking tot het privacybeleid.
Managementteam	Sturing op implementatie privacybeleid.
Functionaris voor Gegevensbescherming	Ziet toe, adviseert en monitort minimaal conform art. 39 AVG.
Informatiebeveiliging & Privacy Forum	Coördinatie omtrent informatiebeveiliging en privacy.
Privacy Officer	Dagelijkse aanspreekpunt, coördinatie, implementatie, informatieverstrekking, risico- analyse, bewustwording, controle en planvorming privacy.
Medewerkers	Gedrag en naleving.
Bestuurszaken/team P & O	Personele zaken.
Informatiemanagement/ team Facilitair	Fysieke toegangsbeveiliging.
Informatiemanagement	Technische beveiliging van informatie.
Ketenpartners en leveranciers	Compliance.

2.4 Reikwijdte

- Het privacybeleid binnen de gemeente geldt voor alle bestuurders, medewerkers (incl. stagiaires, vrijwilligers en gedetacheerden e.d.) en externe relaties (inhuur/outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle middelen waarmee geautoriseerde toegang tot het netwerk van de organisatie verkregen kan worden.
- De nadruk van het beleid ligt op de, geheel of gedeeltelijk, geautomatiseerde/ systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de gemeente evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- Het privacybeleid omvat de gehele ‘data life cycle’; van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan. Het is van toepassing op de verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd. Het beleid is ook van toepassing op beveiligingsproblemen. (‘meldplicht datalekken’).
- Privacybeleid binnen de gemeente heeft raakvlakken met andere beleidsthema’s of vertoont hiermee overlap zoals:
    - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
    - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding, vertrouwensfuncties en integriteit.
    - Informatiebeveiligingsbeleid.
    - Informatiebeleid.

Van belang hierbij is dat de doelen van de privacywetgeving worden behaald.

3 UITGANGSPUNTEN

3.1 Algemene beleidsuitgangspunten
De belangrijkste beleidsuitgangspunten bij de gemeente zijn:

- Het privacybeleid wordt proactief gevoerd op basis van dit beleidskader.
- De verwerking van persoonsgegevens is altijd gebaseerd op één van de wettelijke grondslagen. Hierbij is een goede balans tussen het belang van de gemeente om persoonsgegevens te verwerken en het belang van de betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang.
- Binnen de gemeente is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten en verbale uitlatingen.
- De gemeente is eigenaar van de informatie die onder haar verantwoordelijkheid door derden (verwerkers) wordt verwerkt. Deze verwerkers moeten goed geïnformeerd worden over de regelgeving rond het verwerken van deze informatie.
- De gemeente voert de wettelijke verplichtingen voor gemeentelijke administraties en diensten uit ten behoeve van haar burgers. De gemeente adviseert daarom de burger over de legitimiteit van de verwerking.
- De gemeente stelt met iedere verwerker (bijv. ketenpartners) een overeenkomst op waarin eenduidige afspraken zijn vastgelegd met betrekking tot de verwerking van (persoons)gegevens. Deze wordt vastgelegd in de contractenbank.
- Er wordt van alle medewerkers, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘correct’ gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. De gemeente zal hiervoor een gedragscode formuleren, vaststellen en implementeren.
- Privacy is samen met onder andere informatiebeveiliging bij de gemeente een proces van continue verbetering, waarbij tenminste eenmaal per jaar wordt geëvalueerd. Dit vindt plaats in het IB&P forum en wordt ter vaststelling voorgelegd aan het directieteam en het College van B&W. De raad wordt periodiek op de hoogte gesteld van de voortgang.
- Bij nieuwe diensten en wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen wordt bij de gemeente vanaf de start rekening gehouden met privacy en informatiebeveiliging.

3.2 Risicobeoordeling en risicoafweging
Informatie heeft een waarde: financieel, economisch maar ook emotioneel. De informatie wordt op basis van waarde door de gemeente geclassificeerd. Deze classificatie is het uitgangspunt voor de te nemen maatregelen. Er is een balans tussen de risico’s van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.

3.3 Privacy verplichtingen uit de Algemene Verordening Gegevensbescherming
De gemeente als uitvoerend orgaan van de wettelijke verplichtingen voor gemeentelijke administraties en diensten ten behoeve van haar burgers, hanteert en toetst de regels uit de Algemene Verordening Gegevensbescherming met betrekking tot de omgang met persoonsgegevens. Als uitgangspunt hiervoor is uitgegaan van de Privacy Baseline van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Hieronder volgen de belangrijkste punten uit de Algemene Verordening Gegevensbescherming.

3.3.1 Doelbepaling en doelbinding
Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

- De gemeente verwerkt alleen persoonsgegevens wanneer er sprake is van doel en doelbinding. De gemeente controleert bij aanvang- en gedurende de dienstverlening of hieraan wordt voldaan.
- Verzamelde gegevens mogen niet hergebruikt worden voor andere verwerkingen als dit niet in lijn met het originele doel of er geen grondslag voor is.
- Gegevens moeten een referentie hebben naar de bron waaruit te herleiden is wie de eigenaar van de data is.
- Doel en doelbinding dienen vastgelegd te worden in het register van verwerkingsactiviteiten.

3.3.2 Grondslag
Verwerking van persoonsgegevens mag alleen, indien gebaseerd op een van de zes wettelijke grondslagen.

- De gemeente controleert bij aanvang en gedurende de dienstverlening of hieraan wordt voldaan.
- De gemeente verwerkt slechts persoonsgegevens indien minimaal aan een van de volgende grondslagen wordt voldaan:
  - Toestemming van de betrokkene
  - Noodzakelijk voor de uitvoering van een overeenkomst
  - Noodzakelijk om te voldoen aan een wettelijk verplichting
  - Noodzakelijk om de vitale belang van de betrokkene te beschermen
  - Noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag.
  - Noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde

- De grondslag dient vastgelegd te worden in het register van verwerkingsactiviteiten.

3.3.3 Dataminimalisatie
Bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. De hoeveelheid en het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken en dient in verhouding te staan tot het doel (proportionaliteit). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Er dient eerst gekeken worden of een minder ingrijpend middel voor de hand ligt om een doel te kunnen bereiken (subsidiariteit).

- De gemeente controleert bij aanvang- en gedurende de dienstverlening of het doel niet met minder, alternatieve of andere gegevens kan worden bereikt.
- Er dient bij persoonsgegevens te worden uitgegaan van het ‘Minimum is het Maximum’ principe.
- Het type persoonsgegevens noodzakelijk voor de verwerking dient vastgelegd te worden in het register van verwerkingsactiviteiten.

3.3.4 Bewaartermijnen
Persoonsgegevens mogen niet langer bewaard worden dan strikt noodzakelijk voor de dienstverlening of wettelijke verplichting.

- De gemeente stelt voor iedere verwerking de (wettelijke) bewaartermijnen van persoonsgegevens vast.
- Maatregelen worden getroffen om persoonsgegevens tijdig te verwijderen, vernietigen of te annonimiseren.
- Er wordt actief gemonitord op naleving.
- Bewaartermijnen dienen vast gelegd te worden in het register van verwerkingsactiviteiten.

3.3.5 Inzagerecht en transparantie
Aan betrokkenen dient op transparante wijze verantwoording afgelegd te worden over het gebruik van hun persoonsgegevens, alsmede over het gevoerde privacybeleid. Daarnaast hebben deze betrokkenen recht op inzage, verbetering, aanvulling, verwijdering, beperking of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

- De gemeente richt haar dienstverlening zodanig in dat de ze op transparante wijze verantwoording kan afleggen naar de betrokkenen.
- De processen en informatiesystemen worden door de gemeente zo ingericht dat inzage, verbeteringen, aanvullingen, verwijderingen en afschermingen van persoonsgegevens voor betrokkenen mogelijk is.
- Dit privacybeleid maakt hier integraal onderdeel van uit.
- Er is een proces ingericht waarbij de gemeente bij verzet, inzage, verbeteringen, aanvullingen, verwijderingen en afscherming de betrokkene naar de juiste afdeling en/of verantwoordelijke verwijst.

3.3.6 Data-integriteit
Er moeten maatregelen getroffen worden om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

- De gemeente zorgt ervoor dat de te verwerken persoonsgegevens juist en actueel zijn.
- De gemeente maakt procesbeschrijvingen en afspraken met ketenpartners om dit te waarborgen.
- Beveiliging van gegevens wordt gewaarborgd in het informatiebeveiligingsbeleid.

3.3.7 Profilering
De gemeente respecteert het recht van burgers en medewerkers om niet te worden onderworpen aan een louter op geautomatiseerde verwerking gebaseerd besluit.

- De gemeente doet niet aan louter geautomatiseerde besluitvorming of profilering welke herleidbaar is tot het individu.

3.3.8 Dataportabiliteit
Burgers en medewerkers hebben het recht op dataportabiliteit (de burger of medewerker moet zijn of haar data kunnen meenemen naar een andere dienst) en hebben het recht een kopie te ontvangen van persoonsgegevens die over deze persoon zijn verzameld.

- Op basis van een gegrond verzoek stelt de gemeente data beschikbaar in het kader van dataportabiliteit.
- De gemeente levert op verzoek een kopie van de verzamelde persoonsgegevens aan de burger of medewerker.

3.3.9 Vergeetrecht
Burgers en medewerkers hebben het recht om ‘vergeten’ te worden. Dat wil zeggen dat ze het recht hebben om zich te laten verwijderen uit bestanden, tenzij wettelijke vereisten dit voorkomen.

- De gemeente zal de processen en informatie systemen van de gemeente zo inrichten dat burgers en medewerkers ‘vergeten’ kunnen worden mits er geen wettelijke beperking op rust.
- Gegevens moeten kunnen worden gewist of niet herleidbaar geannomiseerd worden.

3.3.10 Beveiliging
Persoonsgegevens moeten adquaat beschermd worden tegen veropenlijking, diefstal, verandering, vernietiging of ontoegankelijkheid. Hiervoor dient een organisatie afdoende maatregelen te treffen.

- Er is een informatiebeveiligingsbeleid.
- Er behoort een inventarisatie te zijn van de te beveiligen informatie op basis van locatie, risico en waarde.
- Er behoort te worden bewerkstelligd dat de gemeente minimaal de Baseline Informatiebeveiliging Overheid (BIO), de opvolger van de BIG, volgt.
- De gemeente eist van partijen in de gehele keten minimaal een gelijkwaardige norm voor informatiebeveiliging.

3.3.11 Accountability
Organisaties welke persoonsgegevens verwerken moeten een actief beleid voeren en maatregelen treffen waaruit blijkt dat de AVG aantoonbaar wordt nageleefd.

- De gemeente voert een actief privacybeleid en treft maatregelen waaruit men kan aantonen dat de Algemene Verordening Gegevensbescherming continue wordt nageleefd. Het is niet voldoende enkel passief te acteren.
- De gemeente dient onder andere processen, incidenten, besluiten en afwegingen te documenteren.

3.3.12 Privacy by Design & by Default
Bij het ontwikkelen of vernieuwen van informatie systemen en diensten dient privacy vanaf het ‘design’ te worden meegenomen. Bij ‘default’ zijn de instelling zodanig dat maximale privacy wordt betracht.

- De gemeente zal bij de ontwikkeling of vernieuwing van informatie systemen en diensten privacy by design & by default toepassen.
- De gemeente zal pro-actief deelnemen bij de ontwikkeling van nieuwe diensten door ketenpartners en gemeenschappelijke regelingen waar de gemeente deel van uitmaakt. Hiermee wordt zekergesteld dat privacy en informatiebeveiliging vanaf het begin worden meegenomen in het design en de maximale privacy van burgers en medewerkers wordt gewaarborgd.

3.3.13 Gegevensbeschermingseffectbeoordeling

Een gegevensbeschermingseffectbeoordeling (GEB) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Onder de AVG kunnen organisaties hiertoe verplicht zijn. Hieropvolgend kunnen maatregelen nodig zijn om de risico's van de verwerking te verkleinen. Een GEB is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Dit dient de gemeente zelf te bepalen.

- De gemeente zal pro-actief gegevensbeschermingseffectbeoordelingen initieren voor alle bestaande, nieuwe en gewijzigde verwerkingen waarvoor dit van toepassing is.
- De gemeente zal indien nodig ketenpartners, contractpartners en andere verwerkers hierbij betrekken.
- De gemeente zal niet beginnen met het verwerken van gegevens voordat een uit te voeren GEB is doorlopen.

3.3.14 Verwerkersovereenkomsten

De gemeente zorgt ervoor dat bij verwerkingen waarbij persoonsgegevens verwerkt worden de verantwoordelijkheden en eisen met betrekking tot de verwerking zijn vastgelegd in overeenkomsten met de verwerkers.

- De gemeente zal bij iedere nieuwe en of bestaande dienst zeker stellen dat de verwerker en of medeverantwoordelijke voldoende maatregelen heeft getroffen waardoor de gemeente haar verantwoordelijkheid kan nemen.
- De details en eisen die gesteld worden aan de verwerking door verwerkers en medeverantwoordelijke zullen eenduidig worden vastgelegd in een verwerkersovereenkomst. Deze verwerkersovereenkomst wordt afgesloten tussen de gemeente en de verwerkers en of medeverantwoordelijken. Hiermee borgen partijen de rechtvaardigheid van de verwerking.
- Er behoort te worden bewerkstelligd dat daar waar verwerkers en of medeverantwoordelijken verwerkingen uitbesteden aan een sub-bewerker er goedkeuring is van de gemeente. Tevens moeten verwerkers en medeverantwoordelijken waarborgen dat deze sub-bewerker aan minimaal dezelfde vereisten voldoet als vastgelegd in de verwerkersovereenkomst tussen de gemeente en verwerker en medeverantwoordelijke. Ook hier geldt dat dit in een verwerkersovereenkomst tussen verwerker/medeverantwoordelijke en de derde partij (sub-bewerker) eenduidig dient te worden vastgelegd.

3.3.15 Register van verwerkingsactiviteiten

Van alle verwerkingsactiviteiten van persoonsgegevens wordt een register bijgehouden. Hierin worden onder andere de doeleinden van de verwerking, categorieën van betrokkenen en persoonsgegevens, derde ontvangers, sub-bewerkers, bewaartermijnen en te nemen maatregelen opgenomen.

- De gemeente houdt een register bij waarin de verwerkingsactiviteiten worden vastgelegd en geactualiseerd.

3.3.16 Classificatie en Risicoanalyse

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van processen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV).

De gemeente:
- Classificeert informatie met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Zorgt voor passende beveiligingsmaatregelen per classificatieniveau.
- Stelt een classificatiebeleid op en draagt dit classificatiebeleid uit binnen de organisatie.

- Dient geschikte samenhangende procedures te ontwikkelen en te implementeren voor de classificering en verwerking van informatie overeenkomstig het classificatiesysteem dat is vastgesteld.

4 PLAN, DO, CHECK en ACT

Privacy en informatiebeveiliging zijn voortdurend in beweging en veranderingen vinden frequent plaats. Regelmatig wordt gecontroleerd of de bestaande maatregelen nog voldoen. Dit geldt voor zowel privacy als informatiebeveiliging, als de aanvullende maatregelen die volgen uit risicoanalyses. Bovendien moet voor al deze maatregelen regelmatig gecontroleerd worden of ze nog goed werken. Het is dan ook een iteratief proces dat een PDCA-cyclus (Plan Do Check Act) doorloopt.

Plan

1. Het privacybeleid is vastgesteld. Dit vormt de basis voor een jaarplan en/of meerjarige termijnagenda.
2. Een jaarplan of meerjarige termijnagenda bevat alle acties die nodig zijn om de beveiliging en processen met betrekking tot privacy en informatiebeveiliging te optimaliseren.

Do

3. De medewerkers voeren de procedures/maatregelen uit conform het beleid en de afspraken uit het jaarplan.
4. Bij elke nieuwe verwerking voert de gemeente indien nodig, een risicoanalyse uit op privacyaspecten.

Check

5. Periodiek beoordeelt de Functionaris voor Gegevensbescherming of er gewerkt wordt conform het beleid en stelt vast of dit nog actueel is.
6. Jaarlijks controleert de algemeen directeur van de gemeente of de maatregelen uit de plannen zijn uitgevoerd.

Act

7. De bevindingen uit controles worden door de Functionaris voor Gegevensbescherming gerapporteerd aan de algemeen directeur.
8. De algemeen directeur van de gemeente stelt aan de hand van incidenten, meldingen en bevindingen uit controles, verbetermaatregelen vast voor het komende jaar.

5 ORGANISATIE: TAKEN & VERANTWOORDELIJKHEDEN

5.1 Organisatie

Randvoorwaardelijk voor de PDCA-cyclus voor privacy is het organiseren ervan. Uiteindelijk moeten eerst mensen taken, verantwoordelijkheden en bevoegdheden krijgen voordat de stappen uit de PDCA-cyclus gezet kunnen worden.

5.2 Centrale verantwoordelijkheid

Het College van B&W is eindverantwoordelijk voor de naleving van privacywetgeving en voert proactief privacybeleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat dit evenwichtig plaatsvindt. Dat wil zeggen; behoorlijk, zorgvuldig en in overeenstemming met de wet.
De algemeen directeur/gemeentesecretaris is ambtelijk verantwoordelijk voor de kaderstelling en sturing met betrekking tot het beleid.
Het managementteam voert de regie en houdt toezicht op hun processen op basis van dit privacybeleidskader. Het management is operationeel eindverantwoordelijk voor de uitvoering van de hun toegewezen processen.
Het verantwoordelijke gezag stelt hiervoor beleid op, draagt het uit, wijst taken, verantwoordelijkheden en bevoegdheden toe, en bewaakt de gang van zaken.

5.3 Rollen (Functies) rondom Privacy en Informatiebeveiliging

5.3.1 De algemeen directeur/gemeentesecretaris

De algemeen directeur/gemeentesecretaris:

- Stuurt op organisatierisico's en KPI's,

- Beoordeelt of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen.
- Evalueert/beoordeelt periodiek het privacybeleid op basis van evaluatie en aangedragen aanpassingen van het beleid.
- Zorgt dat de Functionaris voor Gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- Verzorgt een actieve ambassadeurs functie voor privacy en toont hierbij voorbeeldgedrag.

5.3.2 Het managementteam

Het managementteam:

- Voert de gedelegeerde verantwoordelijkheden van de algemeen directeur/ gemeentesecretaris uit.
- Stuurt op de implementatie van het privacybeleid.
- Verzorgt een actieve ambassadeurs functie voor privacy en toont hierbij voorbeeldgedrag.

5.3.3 De Functionaris voor Gegevensbescherming (FG):

De FG is binnen de gemeente onafhankelijk toezichthouder op de toepassing van de AVG en geeft op basis van zijn deskundigheid advies. De FG levert een belangrijke bijdrage aan juist gebruik van persoonsgegevens door de organisatie. Deze is aangewezen door het College van B&W op grond van zijn professionele kwaliteiten, deskundigheid op het gebied van de wetgeving en de praktijk en wordt betrokken bij al hetgeen verband houdt met de bescherming van persoonsgegevens en is verplicht tot geheimhouding en vertrouwelijkheid.
De FG:

- Informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens.
- Ziet toe op de naleving van wet- en regelgeving en het door het College van B&W vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens en rapporteert hierover jaarlijks aan de algemeen directeur/gemeentesecretaris.
- Beoordeelt periodiek het privacybeleid op basis van de evaluaties en input van andere stakeholders
- Ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens.
- Geeft advies over Gegevensbeschermingseffectbeoordelingen.
- Werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens.
- Is contactpersoon voor burgers en medewerkers in het geval van privacyvraagstukken.
- Verzorgt een actieve ambassadeurs functie voor privacy en toont hierbij voorbeeldgedrag.
- Kan, indien noodzakelijk, rechtstreeks rapporteren aan het College van B&W.

De FG krijgt de nodige ruimte voor professionele uitvoering van taken.

- De FG wordt naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens.
- De FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- Het College van B&W en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De FG kan vrij en onafhankelijk advies geven.

5.3.4 Informatiebeveiliging en Privacy Forum

Een belangrijk doel van het forum is het elkaar informeren over en afstemmen van ontwikkelingen op het gebied van informatiebeveiliging en privacy. Tevens is voortgang van de implementatie van de maatregelen met betrekking tot informatiebeveiliging en privacy een vast en belangrijk onderwerp. Het Informatiebeveiliging en Privacy Forum verzorgt de coördinatie omtrent informatiebeveiliging en privacy.

5.3.5 Privacy Officer

De Privacy Officer is belast met de dagdagelijkse activiteiten rondom privacy. De Privacy Officer maakt deel uit van het Informatiebeveiliging en Privacy Forum.

De Privacy Officer:

- Voert het privacy jaarplan uit.
- Levert samen met het Platform Privacy en Informatiebeveiliging input aan het jaarplan.

- Evalueert in samenspraak met de Werkgroep Informatiebeveiliging en Privacy het privacybeleid en doet voorstellen tot aanpassingen van het beleid, (PDCA Cyclus).
- Doet voorstellen tot specifieke implementaties.
- Zorgt voor afstemming en bewaakt de voortgang van de activiteiten van het team.
- Zorgt dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- Maakt afspraken met andere organisatieonderdelen over het borgen van de privacy in geval van informatie die stroomt tussen verschillende organisatieonderdelen.
- Zorgt voor naleving van wet-, regelgeving en het privacybeleid (rechtmatige, behoorlijke en transparante verwerking, bewustwording, gebruikt en evalueert GEB's, past 'Privacy bij design/default' toe, zorgt voor registratie van verwerkingsactiviteiten, etc.),
- Verzorgt een actieve ambassadeurs functie voor privacy en toont hierbij voorbeeldgedrag.

6 MIDDELEN

De middelen voor de kosten die verband houden met de uitvoering van het privacybeleid zijn in de begroting opgenomen.

7 CONTROLE EN RAPPORTAGE

Privacy is een continu proces. De Functionaris voor Gegevensbescherming zal, middels controle, erop moeten toezien dat de organisatie continu in controle is. De FG dient de gehele keten te overzien en rekening te houden met externe partijen die in opdracht persoonsgegevens verwerken.

7.1 Rapportage

Over incidenten, status, voortgang en veranderingen met betrekking tot privacy dienen de volgende belanghebbende, middels rapportage, afdoende te worden geïnformeerd:

- College van B&W
- Algemeen directeur/gemeentesecretaris
- Managementteam
- Interne organisatie
- Autoriteiten

Voor externe partijen, die gegevens voor de gemeente verwerken geldt dat zij incidenten, status, voortgang en veranderingen aan de gemeente dienen te melden conform de gemaakte afspraken.