voerendaal
\ gemeente
voerendaal

GEMEENTEBLAD

Officiële uitgave van de gemeente Voerendaal

Nr. 100580
14 mei
2018

Privacybeleid 2018 - 2021

DOCUMENTMANAGEMENT

0.1 Vaststelling en periodieke actualisering

Dit document, het Privacybeleid, wordt vastgesteld door het College van B&W.
Wijzigingen en aanvulling worden aangedragen en verwerkt daar de adviseur Privacy en Informatiebeveiliging. Toetsing en advisering vindt plaats door de Functionaris voor Gegevensbescherming. Vaststelling geschiedt dan via Management door het College van B&W.
Dit beleid wordt vastgesteld voor een periode van 4 jaar en daar waar wettelijke eisen of veranderde inzichten hiertoe aanleiding geven, zal dit beleid worden aangepast.

1 INLEIDING

1.1 Algemene toelichting

Onze inwoners, onze gemeenschap, dat zijn de mensen waar wij voor werken. Deze mensen staan centraal. Soms raken wij met onze dienstverlening direct de kwaliteit van hun leven. Op andere momenten zijn zij op ons aangewezen, maar is de impact minder groot of de vraag minder urgent.
Binnen de gemeente Voerendaal wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke 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 gegevens en privacy. De gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.
Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy.
De gemeente Voerendaal 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 Voerendaal 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 gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. 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 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 is van privacy, het zorgvuldig omgaan met (persoons)gegevens is noodzakelijk voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk.

Een ander belangrijk aspect bij Privacy en Informatiebeveiliging is Informatiemanagement. Informatiemanagement 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 Privacy en Informatiebeveiliging.

2 DOEL EN REIKWIJDTE

2.1 Ambitie

De gemeente wil bijdragen aan een betrouwbare overheid. Burgers moeten erop kunnen vertrouwen dat gemeenten zorgvuldig met hun gegevens omgaan. 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 optimaal niveau van Privacy 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 missie van de gemeente Voerendaal:

De gemeente stelt de privacy en beveiliging van gegevens van burgers, medewerkers en organisaties voorop bij de verwerking van 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

Dit beleid heeft als doelen:

- Het garanderen van de privacy van burgers, organisaties en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden beperkt.
- Het waarborgen van de continuïteit van de dienstverlening en de bedrijfsvoering van de gemeente.
- Het voldoen aan actuele wet- en regelgeving omtrent Privacy
- Privacy integraal onderdeel van de bedrijfsvoering laten zijn.
- Medewerkers te ondersteunen en kennis met betrekking tot Privacy up-to-date te houden.
- Afspraken over de verwerking en beveiliging van (persoons)gegevens, tussen betrokken partijen in de gehele keten middels overeenkomsten te borgen.
- De kwaliteit van de verwerking van informatie en de beveiliging van (persoons)gegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid.
- Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van burgers en medewerkers, wordt gerespecteerd en de gemeente voldoet aan relevante wet- en regelgeving.

2.3 Doelgroep

Dit beleid is van toepassing op de uitvoering van alle taken en heeft betrekking op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, en de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd om daarin te worden opgenomen. Het Privacybeleid is bedoeld voor alle interne en externe medewerkers van de gemeente en inhuurmedewerkers bij de gemeente.

Doelgroep	Relevantie beleid
College van B&W	Integrale verantwoordelijkheid en vaststellen beleid
Algemeen Directeur	Verantwoordelijk voor kaderstelling en sturing mbt beleid
Management	Uitvoering en controle op naleving
Functionaris voor Gegevensbescherming	Controle op naleving en advies op het gebied van Privacy en Informatiebeveiliging
Adviseur Privacy en informatiebeveiliging	Dagelijkse coördinatie, informatieverstrekking, risico- analyse, aanspreekpunt voor privacyvraagstukken bewustwording, controle en planvorming Privacy

Platform Privacy en informatiebeveiliging	Informatieverstrekking, bewustwording, controle en planvorming Privacy en Informatiebeveiliging
Medewerkers	Gedrag en naleving
Proces eigenaren	Sturing op implementatie en controle op naleving
Applicatie beheerders	Sturing op implementatie en controle op naleving
HRM	Personele zaken m.b.t. integriteit medewerkers en functie eisen
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT	Technische beveiliging
Ketenpartners en leveranciers	Compliance

2.4 Reikwijdte

- Het Privacybeleid binnen de gemeente geldt voor alle bestuurders, medewerkers, (incl. stagiaires, vrijwilligers en gedetacheerden e.d.), (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle middelen van waar geautoriseerde toegang tot het netwerk van de organisatie verkregen kan worden.

- De nadruk van het beleid ligt op diensten/verwerkingen, die de gemeente aan de burgers aanbiedt. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de organisatie wordt verwerkt en/of zelf is gegenereerd, en wordt beheerd.

- In het beleid ligt de nadruk 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.

- Privacybeleid binnen de gemeente heeft raakvlakken met:

- 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 en vertrouwensfuncties.

- IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen.

- Informatiebeveiligingsbeleid

- Informatiemanagement

3 UITGANGSPUNTEN

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij de gemeente zijn:

- De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen (publiekrechtelijke taak). Waarbij een goede balans tussen het belang van de gemeente om persoonsgegevens te verwerken en het belang van betrokkene (burger) om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.

- 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 gebruik 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 heeft met iedere verwerker een overeenkomst waarin eenduidige afspraken zijn vast gelegd met betrekking tot de verwerking van (persoons)gegevens.

- De gemeente sluit met alle leveranciers, conform het Privacy en Informatiebeveiligingsbeleid, verwerkersovereenkomsten af als zij (persoons)-gegevens ontvangen en verwerken van de ge-

meente. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van burgers of medewerkers worden verstrekt, al dan niet op wettelijke basis.

- 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 heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Privacy is naast Informatiebeveiliging bij de gemeente een proces van continious improvement, waarbij regelmatig wordt geëvalueerd.
- 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. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van deze classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.

Voor het afwegen van risico's ten aanzien van privacy zijn methoden beschikbaar zoals het uitvoeren van een nulmeting, eventueel gevolgd door een diepgaande risicoanalyse, en een Gegevensbeschermingseffectbeoordeling (GEB).

3.3 Uitgangspunten Privacy
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. 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 doelbindingen dienen vastgelegd te worden in het verwerkingenregister.

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.
- Er dient te worden gecontroleerd of de verwerking aan minimaal een van de volgende grondslagen voldoet:

- Toestemming
- Overeenkomst
- Wettelijk verplichting

- Publiekrechtelijke taak
- Vitaal belang van de betrokkene
- Gerechtvaardigd belang

- De grondslag dient vastgelegd te worden in het verwerkingenregister.

3.3.3 Dataminimalisatie
Bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het aantal en het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze moet staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.

- De gemeente controleert bij aanvang- en gedurende de dienstverlening of het doel niet met minder, alternatieve of andere gegevens kan worden bereikt.
- Er dient te worden uitgegaan van het “Minimum is het Maximum” principe.
- Het type persoonsgegeven(s) noodzakelijk voor de verwerking dient vastgelegd te worden in het verwerkingenregister.

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 dienen getroffen te worden om persoonsgegevens tijdig te verwijderen, vernietigen of te annonimiseren.
- Er dient actief te worden gemonitord op naleving.
- Bewaartermijnen dienen vast gelegd te worden in het verwerkingenregister.

3.3.5 Inzagerecht en transparantie
Aan betrokkenen (burgers, medewerkers en organisaties) 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 wordt 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 dient procesbeschrijvingen en afspraken met ketenpartners te maken om dit te waarborgen.
- Beveiliging van data dient gewaarborgd te zijn in het informatie- beveiligingsbeleid.

3.3.7 Profilering
Het recht van burgers en medewerkers om niet te worden onderworpen aan een louter op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit wordt gerespecteerd.

- 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 hem zijn verzameld.

- Er dient te worden bewerkstelligd dat de gemeente op basis van een gegrond verzoek data beschikbaar stelt in het kader van dataportabiliteit.
- Er dient te worden bewerkstelligd dat de gemeente op verzoek een kopie van de verzamelde persoonsgegevens aan de burger of medewerker kan leveren.

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 geanonimiseerd 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 behoort een informatiebeveiligingsbeleid te zijn.
- 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 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 en 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
Omdat het verwerken van persoonsgegevens tot de kernactiviteiten van gemeenten behoort, stelt de Autoriteit Persoonsgegevens het uitvoeren van Gegevensbeschermings-effectbeoordeling (impactanalyse) bij nieuwe en gewijzigde verwerkingen verplicht, om ervoor te zorgen dat de gegevensverwerking op een verantwoorde manier plaatsvindt.

- De gemeente zal pro-actief Gegevensbeschermingseffectbeoordelingen initieren voor alle bestaande, nieuwe en gewijzigde verwerkingen.
- De gemeente zal indien noodzakelijk ketenpartners, contractpartners en andere verwerkers hierbij betrekken.

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 moet worden vastgelegd.

3.3.15 Register van verwerkingen
Van alle verwerkingsactiviteiten van persoonsgegevens per proces 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 WET- EN REGELGEVING

4.1 Wetgevingen

In veel wet- en regelgeving is privacy als onderdeel opgenomen. Een opsomming (niet uitputtend) hiervan is de Algemene Verordening Gegevensbescherming, WOB, BAG, BRP, SUWI, WMO, Jeugdwet, BGT, WKPB, Archiefwet, Wet Computercriminaliteit, Telecommunicatiewet, Auteurswet en overige materiewetten.

4.2 Normenkaders

Als uitgangspunt voor het Privacybeleid is uitgegaan van:

• De Privacy Baseline versie 3.1
Het Centrum Informatie Beveiliging (CIP) heeft een Privacy Baseline opgesteld waarmee de verwerkingsverantwoordelijke kan controleren in hoeverre hij aan privacy wet- en regelgeving voldoet en afwegingen kan maken bij die zaken die hem daarvoor – volgens de Baseline – nog te doen staan.

5. PLAN, DO, CHECK en ACT

Privacy en Informatiebeveiliging is 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 beleid Privacy 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 m.b.t. 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 een risicoanalyse uit op privacyaspecten.
Check
5. Periodiek controleert 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.

6 ORGANISATIE: TAKEN & VERANTWOORDELIJKHEDEN

6.1 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.

6.2 Centrale verantwoordelijkheid

Het College van B&W is eindverantwoordelijk voor privacy en informatieveiligheid. De algemeen directeur is verantwoordelijk voor de kaderstelling en sturing met betrekking tot het beleid en het management zorgt voor uitvoering en controle op naleving.
Het verantwoordelijke gezag stelt hiervoor beleid op, draagt het uit, wijst taken, verantwoordelijkheden en bevoegdheden toe, en bewaakt de gang van zaken.

6.3 Rollen (Functies) rondom Privacy en Informatiebeveiliging
6.3.1 De algemeen directeur
De algemeen directeur:
- Stuurt op organisatierisico's,
- Beoordeelt of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen.
- Beoordeelt periodiek het Privacybeleid op basis van de evaluatie en aanpassingen van het beleid en plan van het Privacy en Informatiebeveiligingsteam.
- 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.

6.3.2 De Functionaris voor gegevensbescherming (FG):
De FG is binnen de gemeente onafhankelijk toezichthouder op de toepassing van de AVG en krijgt geen instructies over de uitvoering van de taken. 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 alles wat 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.
- 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.
- Mag indien noodzakelijk, rechtstreeks rapporteren aan het College van B&W.

6.3.3 Platform Privacy en Informatiebeveiliging
Een Platform Privacy en Informatiebeveiliging wordt geformeerd. Het team zal naast een coördinator bestaan uit een vaste kern en een flexibel deel van leden. Leden van het Platform Privacy en Informatiebeveiliging zijn doorgaans verantwoordelijk voor processen, applicaties, infrastructuur of interne diensten zoals administraties en personeelszaken. Afhankelijk van de noodzaak en situatie maakt een lid deel uit van de kern of het flexibele deel van het team.

Leden van het Platform Privacy en Informatiebeveiliging:
- Dragen middels hun specifieke expertise bij aan het opzetten en onderhouden van het beleid en beleidsplan.
- Signaleren risico's en tekortkomingen ten aanzien van het beleid. (PDCA)
- Zijn het eerste aanspreekpunt binnen de organisatie.
- Fungeren als ambassadeur en coach op de werkvloer.

- Doen aanbevelingen op het gebied van Privacy en Informatiebeveiliging.
- Rapporteren aan de adviseur Privacy en Informatiebeveiliging en aan de algemeen directeur.

6.3.4 Adviseur Privacy en Informatiebeveiliging
De adviseur Privacy en Informatiebeveiliging maakt deel uit van het Privacy en Informatiebeveiligingsteam en draagt zorg voor de coördinatie hiervan.

De adviseur Privacy en Informatiebeveiliging:
- Voert het Privacy en Informatiebeveiligingsjaarplan uit.
- Levert samen met het Privacy en Informatiebeveiligingsteam input aan het jaarplan.
- In samenspraak met het Privacy en Informatiebeveiligingsteam opstellen en evalueren van het Privacy en Informatiebeveiligingsbeleid, opstellen van voorstellen tot implementatie en aanpassingen van het beleid, (PDCA Cyclus)
- 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 en Informatiebeveiliging 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 PIA's, past 'Privacy bij design/default' toe, zorgt voor registratie van verwerkingsactiviteiten, etc.),

6.4 Autoriteit Persoonsgegevens (AP)
Er is sprake van een datalek als er inbreuk is op de beveiliging van persoonsgegevens. Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of (gerede kans op) onrechtmatige verwerking. Indien een datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (betrokkene) dient het datalek gemeld te worden aan de Autoriteit Persoonsgegevens.
Organisaties dienen te beschikken over een functionaris die datalekken meldt en verdere communicatie en opschaling stroomlijnt. Bij de gemeente is dat de FG.

7 MIDDELEN
De middelen voor de kosten die verband houden met de uitvoering van het Privacy en Informatiebeveiligingsplan zijn in de begroting opgenomen.

8 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. Hij dient de gehele keten te overzien en rekening te houden met externe partijen die in opdracht persoonsgegevens verwerken.

8.1 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
- Management
- Accountant
- 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.