Gemeente Roosendaal

GEMEENTEBLAD

Officiële uitgave van de gemeente Roosendaal

Nr. 154726

7 april

2023

Privacybeleid gemeente Roosendaal 2023 – 2025

Burgemeester en wethouders van de gemeente Roosendaal;

gelet op de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming en de Wet politiegegevens (Wpg).

BESLUITEN

vast te stellen **het Privacybeleid gemeente Roosendaal 2023-2025**.

1. Inleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing. De AVG zorgt samen met de Uitvoeringswet AVG onder andere voor versterking en uitbreiding van de privacy rechten voor betrokkenen met meer verplichtingen en verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.

De AVG legt de verantwoordelijkheid bij ons als organisatie om aan te tonen dat wij aan de privacyregels voldoen, de zogenaamde verantwoordingsplicht (accountability). Door hieraan te voldoen leveren wij een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Dit privacybeleid is ook gericht op de Wet politiegegevens (hierna: Wpg). De Wpg is in 2019 aangepast aan de hand van Europese richtlijnen. Op basis van deze wetgeving houdt de Functionaris gegevensbescherming (FG) ook toezicht op het verwerken van politiegegevens door medewerkers van de gemeente. Dit zijn de boa's (buitengewoon opsporingsambtenaren) en de leerplichtambtenaren.

Volgens de AVG en de Wpg moet de gemeente transparant weergeven welke persoonsgegevens zij verwerkt[1] en voor welk doel. Binnen de gemeente Roosendaal wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verwerkt voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met die persoonsgegevens omgaat. 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 en transparantie.

De gemeente Roosendaal geeft met dit privacybeleid een duidelijke richting aan privacy en laat zien dat zij privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente en op processen die worden uitgevoerd door leveranciers. Dit privacybeleid is in lijn met de relevante Europese, nationale, regionale en lokale wet- en regelgeving.

2. Wettelijk kader

Verwerkingen van persoonsgegevens zijn gebonden aan wet- en regelgeving. In deze wet- en regelgeving staan bepalingen die aangeven hoe met de bescherming van persoonsgegevens moet worden omgegaan. De belangrijkste wettelijke kaders staan in:

- Wet politiegegevens
- Artikel 8 Europese Verdrag voor de Rechten van de Mens;
- Artikelen 10 t/m 13 Grondwet;
- De Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG;
- Wetten gericht op de uitvoering in specifieke sectoren zoals:
  - Wet Maatschappelijke Ondersteuning 2015;
  - Jeugdwet;

1) Het begrip 'verwerken' is erg ruim en betekent eigenlijk alles wat met persoonsgegevens gedaan wordt. Naast het verzamelen of vernietigen van persoonsgegevens is ook al het raadplegen van persoonsgegevens een verwerking waarbij op de regels van de AVG gelet moet worden.

  - Wet Algemene bepalingen Omgevingswet (WABO);
  - Wet open overheid (Woo);
  - Wet Basis Registratie Personen (BRP);
  - Alcoholwet;
- Archiefwet;
- Het wetboek van Strafrecht.

3. Uitgangspunten

De gemeente Roosendaal gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

- Inwoners kunnen vertrouwen op onze **zorgvuldigheid**;
  Inwoners, bedrijven en belanghebbenden moeten erop kunnen vertrouwen dat we zorgvuldig met hun gegevens omgaan.[2] Wij zijn een betrouwbare overheid, zeker omdat mensen niet altijd de keuze hebben om hun (soms zeer privacygevoelige) gegevens aan ons te geven;

- We passen **data-minimalisatie** toe;
  De gemeente verwerkt alleen persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. Er wordt gestreefd naar minimale gegevensverwerking.
  We verzamelen alleen als dat noodzakelijk is voor de uitvoering van overheidstaken. Bij het verstrekken wegen wij het individuele belang af tegen het maatschappelijke belang.

- We passen **Privacy-by-design en Privacy-by-default** toe;
  We nemen privacy afwegingen en informatieveiligheidsmaatregelen vanaf het begin mee bij het opzetten en aanpassen van processen en systemen.

- We geven toegang tot informatie volgens het "**Need-to-know**" en "**Need-to-Use**" principe;
  Onze medewerkers mogen en kunnen alleen die gegevens zien die zij voor hun werk nodig hebben.
  We beschermen onze (persoons)gegevens tegen ongeoorloofde toegang;

- We **informeren betrokkenen**;
  We informeren betrokkenen over de persoonsgegevens die wij van hen verwerken en de reden hiervoor. Dit noemen we transparantie. Vaak gebeurt dit al doordat de betrokkene zijn/haar gegevens zelf doorgeeft op een aanvraagformulier. Hierop staat vermeld welke persoonsgegevens nodig zijn en voor welk doel. Iedere betrokkene heeft het recht om op te vragen welke persoonsgegevens van hem of haar worden verwerkt. Daarnaast heeft de betrokkene ook het recht om deze gegevens te laten verbeteren, aan te vullen of te verwijderen. Hiervoor kan een verzoek ingediend worden op de gemeentelijke website of persoonlijk bij een balie van Publiekszaken. Identificatie is verplicht, hetzij door inloggen met DigiD of door het tonen van identificatie aan de balie.

- We **beschermen** onze gegevens;
  We beschermen al onze systemen en de gegevens die we daarin verwerken en opslaan volgens de richtlijnen en normen uit de Baseline Informatiebeveiliging Overheid (BIO);

- We nemen maatregelen gebaseerd op **risico acceptatie**;
  We kiezen bij het nemen van informatieveiligheidsmaatregelen voor de juiste balans tussen informatieveiligheid en risico, kosten en gebruiksgemak. Zo voorkomen we dat maatregelen de werkprocessen belemmeren of overbodig zijn;

- We blijven **verantwoordelijk voor persoonsgegevens** "**in huis**" en "**bij derden**";

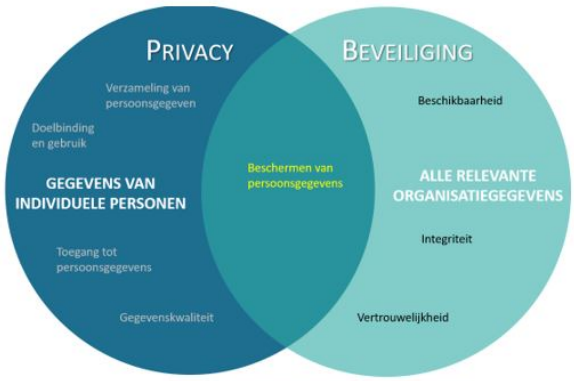
2) AVG artikel 5, lid 1, a.

We zijn ook verantwoordelijk voor de verwerkingen en de informatie die we door “derden” laten uitvoeren. Daar maken we goede afspraken over met de ketenpartners en leveranciers die we in (verwerkers)overeenkomsten vastleggen;

- **Procesbeheerders** zijn verantwoordelijk voor het bijhouden van wijzigingen in het proces;
  We stimuleren procesbeheerders in onze organisatie in het nemen en voelen van verantwoordelijkheid voor de zorg rond privacy en informatieveiligheid.

4. Samenhang Privacy en Informatieveiligheid

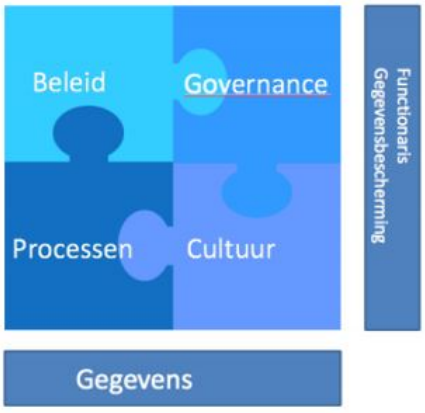
Privacy en Informatieveiligheid zijn twee terreinen die met elkaar verbonden zijn. In de bescherming van persoonsgegevens hebben privacy en informatiebeveiliging ieder een eigen invalshoek. Dit blijkt ook uit de AVG (art. 5, lid 1, f) waarin staat dat persoonsgegevens op een veilige manier verwerkt moeten worden door het nemen van de juiste technische en organisatorische maatregelen. Maatregelen die ervoor moeten zorgen dat het verwerken van persoonsgegevens op een passende beveiliging kan rekenen.



Figuur 1: Samenhang Privacy en Informatieveiligheid

5. Inrichtingsmodel Privacy

In het onderstaande model is aangegeven hoe beleid, governance, processen, cultuur en gegevens zich tot elkaar verhouden. We gebruiken het als een sturingsmodel binnen het werkgebied van Privacy.



Figuur 2: Inrichtingsmodel Privacy

5.1 Beleid

Dit privacybeleid is randvoorwaardelijk voor alle processen waarvoor persoonsgegevens worden verwerkt.
Bij het ontwikkelen van gemeentelijk privacybeleid volgen we daar waar mogelijk landelijk beleid. Het bewaken en handhaven van de privacyregels door gemeenten wordt daardoor vergemakkelijkt.

5.2 Governance

Governance van Privacy

Hoe de Governance rond Privacy wordt uitgevoerd is weergegeven in onderstaande figuur.

Figuur 3 Governancemodel privacy

De Governance is verdeeld in drie niveaus:

1. Niveau 1: gaat over het borgen van de privacy kennis, kunde en aandacht binnen de werkprocessen van de lijn. Proceseigenaren en privacy aanspreekpunten binnen de groepen hebben hierin een belangrijke rol;
2. Niveau 2: de PO zorgt voor beleidsvorming, adviseren en faciliteren van de proceseigenaren.
3. Niveau 3: gaat over het stellen van kaders, onafhankelijk toezicht, strategisch adviseren, toetsen en rapporteren. Dit wordt ingevuld door de FG en CISO.

Overlegstructuren

Aan de directie, het college van burgemeester en wethouders wordt jaarlijks gerapporteerd over de ontwikkelingen rondom privacy en informatieveiligheid. Voordat de rapportage wordt vastgesteld door het college, vindt overleg plaats met de directie.

In 2018 is een werkgroep privacy samengesteld. Aan de werkgroep nemen deel: de FG, PO, CISO, (concern)controller, juridisch adviseur en de teamleider Publiekszaken. De werkgroep overlegt iedere vier weken onder voorzitterschap van de FG. Agendapunten zoals nieuwe wet- en regelgeving, datalekken en andere ontwikkelingen worden besproken, hiervan wordt een verslag gemaakt.

Rollen en verantwoordelijkheden rond Privacy

In de onderstaande tabel zijn de rollen en verantwoordelijkheden met betrekking tot privacy opgenomen.

Rol	**Verantwoordelijk**
College Burgemeester	Verwerkingsverantwoordelijk (eindverantwoordelijk)
Directie	Verantwoordelijk (uitvoering)
Groepen, proceseigenaren	Uitvoerend (procesverantwoordelijk)
Privacy Officer	Adviserend/uitvoerend
Chief Information Security Officer (CISO)	Adviserend/controle
Functionaris Gegevensbescherming (FG)	Toezicht/controle/adviserend

College van B&W

Het college van B&W is verantwoordelijk voor het verwerken van persoonsgegevens binnen de gestelde kaders. Het college stelt hiervoor de beleidskaders en specifieke regelingen en procedures vast. Jaarlijks wordt verantwoording afgelegd aan de gemeenteraad over privacy en de toepassing van het privacybeleid door het vaststellen van de FG jaarrapportage en via de paragraaf bedrijfsvoering in de jaarstukken.

Directie

De directie van de organisatie is voor het bestuur van de gemeente, ambtelijk opdrachtnemer en eindverantwoordelijk voor de uitvoering van de taken in de organisatie rond Privacy. De directie stimuleert de kennisvergaring en bewustwording bij de medewerkers. De directie wijst de medewerkers op hun verantwoordelijkheden ten aanzien van Privacy.

Proceseigenaren
Proceseigenaren zijn de medewerkers die het proces beschrijven en wijzigingen in het proces beheren. De privacy aanspreekpunten van de groepen/teams zien toe op de dagelijkse naleving van de AVG van de processen van de groepen/teams.

Functionaris Gegevensbescherming (FG)
- Ziet toe op de naleving van de AVG en UAVG.
- Is onafhankelijk en kan voor de uitoefening van zijn rol geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die de FG heeft benoemd (artikel 37 AVG).
- Is contactpersoon voor de Autoriteit Persoonsgegevens (AP).
- Houdt toezicht op de opvolging van aanbevelingen die voortvloeien uit Data Protection Impact Assessments (DPIA).
- Rapporteert periodiek aan de directie over de staat van privacy in de organisatie en jaarlijks aan de verantwoordelijken in de gemeente.

Verantwoording Privacy
Op diverse niveaus vindt er door de FG, toezicht en verantwoording plaats over de uitvoering van het privacybeleid.
1. De FG stelt elk jaar een FG rapportage gegevensverwerking op.
2. In de jaarrekening wordt aandacht besteed aan de speerpunten uit de FG rapportage gegevensverwerking.
3. Raadsvragen en informerende presentaties aan de raad. Op verzoek van de raad.
4. Informerende presentatie in de OR. Op verzoek van de OR.
5. Vragen van burgers, journalisten en medewerkers over de wijze waarop gemeente Roosendaal omgaat met privacy.
6. Actuele privacyverklaring op de website (www.roosendaal.nl).

De PO richt zich met name op uitvoerende privacytaken zoals:
1. (het actualiseren van)een AVG-verwerkingsregister,
2. Afhandelen van inzageverzoeken
3. Afhandelen van datalekken
4. Begeleiden en uitvoeren van DPIA's (data protection impact assessment), dit zijn vragenlijsten om privacyrisico's van een gegevensverwerking in kaart te brengen.

5.3 Processen
De processen van de gemeente Roosendaal worden beschreven en vastgelegd. Aan ieder proces wordt een Proceseigenaar gekoppeld. Hiermee is inzichtelijk en controleerbaar onder wiens verantwoordelijkheid het proces wordt uitgevoerd. Het privacy aanspreekpunt van elke groep/elk team zien toe op naleving van de regels van de AVG binnen de processen.

Grondslag en doelbinding
De PO houdt voor de gemeente een actueel verwerkingsregister bij met daarin alle verwerkingen waarin persoonsgegevens worden vastgelegd. Voor elke verwerking is aangegeven wat de wettelijke grondslag is, voor welk doel de persoonsgegevens worden geregistreerd, waar ze vandaan komen, met wie ze worden gedeeld en wat de bewaartermijn is.

Subsidiariteit
Bij de verwerking van persoonsgegevens wordt erop toegezien dat een inbreuk op de persoonlijke levenssfeer van de betrokkenen zoveel mogelijk wordt beperkt. Er wordt altijd nagegaan of het doel ook met minder ingrijpende middelen kan worden bereikt.

Proportionaliteit
De inbreuk op de belangen van betrokkenen mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

Rechtmatigheid, behoorlijkheid, transparantie
De gemeente heeft de processen zo ingericht zodat personen, van wie wij (bijzondere) persoonsgegevens verwerken, hun rechten kunnen uitoefenen. Personen, van wie de gemeente persoonsgegevens verwerkt, worden begrijpelijk geïnformeerd over de verwerking via de privacyverklaring op de website.

Transparantie heeft ook beperkingen wanneer er sprake is van legitieme uitzonderingen. Dit kan zijn in situaties die betrekking hebben op de openbare orde en veiligheid. De gemeente kan, met inachtneming van wet- en regelgeving, een voorbehoud maken op het transparantiebeginsel.

Data Protection Impact Assessments (DPIA)
Wij voeren Data Protection Impact Assessments (DPIA's) uit op verwerkingen die mogelijk een verhoogd risico opleveren. Een Data Protection Impact Assessment is een gegevensbeschermingeffectsbeoordeling waarin eventuele risico's met betrekking tot de verwerking van de persoonsgegevens worden beschreven.

Privacy by Design en Privacy by Default
De gemeente Roosendaal houdt bij de ontwikkeling van processen en systemen rekening met privacy. Bij het ontwerpen denken we na over welke persoonsgegevens noodzakelijk zijn om te registreren en hoe lang deze bewaard moeten worden.

5.4 Bewustwording
Om onze medewerkers privacybewust te laten worden en privacybewust te laten blijven, geven we workshops, trainingen en organiseren we bijeenkomsten.

e-Learning
De gemeente zet in op het gebruik van e-learning als instrument in het bewustmaken van medewerkers in de omgang met informatie. Medewerkers kunnen de modules en instructies op eigen tempo volgen.

Workshops
De FG en de CISO organiseren privacy- en informatieveiligheidsworkshops waarin zij onder andere dieper ingaan op de beginselen van de AVG en wat dit betekent voor de werkzaamheden in de organisatie. Een privacy en informatiebeveiligingstraining is een verplicht onderdeel bij de on boarding van nieuwe medewerkers. Hier worden de medewerkers op de hoogte gebracht van de beginselen van de AVG en het belang van privacy en informatieveiligheid bij het werk dat zij verrichten voor de gemeente Roosendaal.

5.4 Persoonsgegevens
De gemeente gaat zorgvuldig om met persoonsgegevens. De inwoners van de gemeente en ook de medewerkers van de organisatie moeten ervan uit kunnen gaan dat hun persoonsgegevens vertrouwelijk worden behandeld en goed worden beveiligd.

Verwerkersovereenkomsten met derden
De gemeente maakt gebruik van derde partijen bij de uitvoering van werkzaamheden waartoe zij zelf geen mogelijkheden bezit. Hierbij valt te denken aan leveranciers van software, netwerkdiensten, data-opslag. De gemeente maakt alleen gebruik van derde partijen als verwerkers van persoonsgegevens (aantoonbaar) voldoende garanties kunnen bieden om de verwerking van (persoons)gegevens te laten voldoen aan de AVG-vereisten. Hiervoor wordt zoveel mogelijk gebruik gemaakt van de modelovereenkomst van de Vereniging Nederlandse Gemeentes (VNG).

Dataminimalisatie
De gemeente verwerkt alleen die persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. Er wordt gestreefd naar minimale gegevensverwerking.

Bewaartermijn(en)
De gemeente bewaart persoonsgegevens niet langer dan nodig is. Het gebruiken en bewaren van persoonsgegevens kan nodig zijn om gemeentelijke taken goed uit te voeren of om wettelijke verplichtingen na te kunnen leven. Voor de bewaartermijnen wordt zoveel mogelijk aangesloten bij de Archiefwet. Daar waar wet- en regelgeving, zoals de selectielijst, geen uitsluitsel geeft over bewaring van persoonsgegevens, dienen die persoonsgegevens volgens de AVG niet langer bewaard te worden dan nodig is en direct te worden vernietigd.

6. Afsluiting
Het beleid wordt iedere drie jaar geëvalueerd en indien nodig herzien. Dit beleid is te vinden op de website van de gemeente Roosendaal (www.roosendaal.nl/privacy).

Intrekking
Het privacybeleid gemeente Roosendaal, vastgesteld op 22 mei 2018 en het privacybeleid gemeente Roosendaal 2021-2024, vastgesteld op 14 december 2021 worden ingetrokken.

Inwerkingtreding
Dit besluit treedt in werking op de derde dag na bekendmaking in het gemeenteblad.

Aldus besloten door burgemeester en wethouders van Roosendaal op 4 april 2023,
de secretaris, de burgemeester,