Privacybeleid gemeente Rheden
2019-2022

Inhoud

1. Inleiding

Gemeente Rheden maakt veel gebruik van persoonsgegevens. Dit doen wij niet alleen in het kader van dienstverlening naar de inwoners, maar ook als werkgever. Wij vinden het van groot belang dat zorgvuldig wordt omgegaan met deze persoonsgegevens. Inwoners en medewerkers (betrokkenen) hebben hier recht op en moeten hierop kunnen vertrouwen.

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Dit is de opvolger van de Wet bescherming persoonsgegevens (Wbp). De AVG stelt, evenals de Wbp, grenzen aan wat wij met persoonsgegevens mogen doen. Wanneer dit niet wordt nageleefd, kan dit grote gevolgen hebben voor zowel ons als betrokkenen. De grootste veranderingen onder de AVG zijn dat wij meer verantwoording moet kunnen afleggen over de omgang met persoonsgegevens, dat rechten van betrokkenen zijn versterkt en uitgebreid en dat de Autoriteit Persoonsgegevens (AP) meer controle- en handhavingsbevoegdheden heeft.

Het privacybeleid helpt ons om op een zorgvuldige wijze om te gaan met persoonsgegevens en hierbij de juiste keuzes te maken. Zaak is om een juiste balans te vinden tussen het leveren van goede en efficiënte dienstverlening op basis van de gemeentelijke taken en de bescherming van persoonsgegevens hierbij waar onze inwoners ook bij gebaat zijn. Hierbij wordt gekozen voor een risicogerichte werkwijze.

Om persoonsgegevens goed te kunnen beschermen is het belangrijk dat de informatiebeveiliging op orde is. Technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van persoonsgegevens. In een apart informatiebeveiligingsbeleid wordt aangegeven op welke wijze dit geborgd is binnen onze gemeente. Dit informatiebeveiligingsbeleid draagt mede bij aan naleving van dit privacybeleid.

Dit privacybeleid omvat organisatiekeuzes omtrent de omgang met persoonsgegevens, verdeling van rollen en verantwoordelijkheden hierbij en de bijbehorende risico’s met te nemen maatregelen. Hierbij wordt aan een aantal onderwerpen wegens hun gevoelige aard met betrekking tot persoonsgegevens extra aandacht besteed. Enkele onderdelen van het privacybeleid worden in de begrippenlijst verder toegelicht.

Dit beleid is opgesteld door de Privacy Officer (PO) en afgestemd met de Chief Information Security Manager (CISO), de Functionaris voor de Gegevensbescherming (FG) en het team Juridisch Advies. Dit privacybeleid treedt in werking na vaststelling door het College van Burgemeester en Wethouders (College). Het beleid wordt jaarlijks geëvalueerd en indien nodig herzien.

2. Reikwijdte

Dit beleid is van toepassing op alle taken en processen waarbij persoonsgegevens worden gebruikt. Hierbij gaat het niet alleen om de uitvoering van overheidstaken, maar ook om taken die worden uitgevoerd door onze gemeente als werkgever. Dit beleid dient nageleefd te worden door alle medewerkers die persoonsgegevens verwerken en door externe partijen die dit namens ons doen.

3. Juridisch kader

De AVG regelt het algemene kader voor de omgang met persoonsgegevens. De Nederlandse Uitvoeringswet AVG (UAVG) heeft daarnaast een aantal onderwerpen uit de AVG nog wat verder uitgewerkt en strikter geregeld. Verder zijn in tal van bijzondere wetten regels met betrekking tot omgang met persoonsgegevens opgenomen.

4. Uitgangspunten voor beleid

Ter uitvoering van dit beleid worden, om op een verantwoorde wijze met persoonsgegevens om te kunnen gaan, de volgende uitgangspunten gehanteerd:

Gerechtvaardigde grondslag

Persoonsgegevens worden alleen gebruikt wanneer hier een gerechtvaardigde grondslag (rechtsgrondslag) voor is. Bij gemeentelijke dienstverlening mogen persoonsgegevens in beginsel alleen gebruikt worden voor de uitvoering van een wettelijke taak. Gebruik van persoonsgegevens van medewerkers moet in beginsel noodzakelijk zijn voor de uitvoering van een (arbeids)overeenkomst of een wettelijke taak. Wanneer toestemming kan worden gebruikt als grondslag, gebeurt dit alleen met een getekend toestemmingsformulier dat voldoet aan de wettelijke vereisten. Toestemming wordt alleen gebruikt als er geen andere rechtsgrondslag mogelijk is en het wel of niet geven van toestemming besluitvorming niet beïnvloedt. Gebruik van persoonsgegevens zonder grondslag gebeurt alleen nadat de proceseigenaar de belangen goed heeft afgewogen en een risicoanalyse heeft uitgevoerd, maatregelen heeft genomen om de risico's te beperken en goedkeuring heeft gekregen van diens teammanager.

Doelstelling

Aan de hand van de rechtsgrondslag dient een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel te worden vastgesteld die medewerkers met het gebruik van de persoonsgegevens willen bereiken. Persoonsgegevens mogen alleen worden gebruikt voor een ander doel dan dit vastgestelde doel wanneer de wet dit toelaat.

Opvragen en opslag persoonsgegevens

Wanneer medewerkers door van hun werkzaamheden al toegang hebben tot persoonsgegevens (bijvoorbeeld in één van de basisregistraties waartoe de medewerker geautoriseerd is), worden deze niet opnieuw opgevraagd. Persoonsgegevens worden verder op zo min mogelijk locaties opgeslagen en worden niet langer bewaard dan noodzakelijk is of de wet voorschrijft.

Minimalisatie van persoonsgegevens

Bij het gebruik van persoonsgegevens wordt de minst vergaande handelswijze gekozen. Medewerkers gebruiken alleen de persoonsgegevens die zij nodig hebben om hun werkzaamheden goed uit te kunnen voeren (dataminimalisatie) en indien mogelijk worden persoonsgegevens geanonimiseerd of pseudonimiseerd. Persoonsgegevens mogen niet enkel gebruikt worden om het werk te vergemakkelijken. Verder worden persoonsgegevens met zo min mogelijk collega's of externe partners uitgewisseld. Wanneer het noodzakelijk is om persoonsgegevens met externen uit te wisselen, dienen hier de juiste afspraken onder te liggen.

Nieuwe of gewijzigde werkprocessen
Wanneer door nieuwe of gewijzigde werkprocessen persoonsgegevens op een andere manier gebruikt gaan worden dan voorheen, dienen de noodzakelijke en wettelijk verplichte stappen te worden gezet om het werkproces zo in te richten dat het aan de privacywetgeving voldoet.

Afhandeling verzoeken, meldingen en klachten
Betrokkenen kunnen op grond van de AVG bepaalde rechten inroepen. Deze zijn gecommuniceerd via onze website in een privacyverklaring. Middels een formulier via de website of per brief kan hiertoe een verzoek worden ingediend. Het verzoek wordt via een apart vastgestelde procedure binnen de juiste termijnen afgehandeld. Ook kunnen betrokkenen meldingen en klachten indienen over het gebruik van hun persoonsgegevens door ons. Deze worden doorgezonden aan de PO of FG voor een juiste afhandeling.

Datalekken
Het gebruik van persoonsgegevens is mensenwerk en er kan onverhoopt iets misgaan. Dit kan resulteren in een datalek. Indien een medewerker hiermee te maken krijgt, wordt dit gemeld via het speciaal daarvoor ingerichte formulier. Het incident wordt vervolgens afgehandeld volgens een aparte vastgestelde procedure en hierbij wordt alles gedaan wat in onze macht ligt om (mogelijke) negatieve gevolgen voor betrokkenen zoveel mogelijk te beperken.

Bewustwording en communicatie
Het is van belang dat medewerkers weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Wij ondersteunen dit door te zorgen voor periodieke trainingen en richtlijnen. Verder worden bewustwordingsacties uitgezet om het belang van naleving van dit privacybeleid extra te benadrukken. Wij streven verder een cultuur na waarbij medewerkers elkaar aan kunnen spreken op gedrag omtrent de omgang met persoonsgegevens.

Betrokkenen hebben het recht te weten wat met diens persoonsgegevens gebeurt. Hiertoe is een privacyverklaring opgesteld, welke is gepubliceerd op onze website. Wanneer persoonsgegevens worden verwerkt op basis van toestemming, gebeurt dit middels een toestemmingsverklaring waarop duidelijk wordt aangegeven welke persoonsgegevens waarvoor zullen worden gebruikt en voor welk doel. Wanneer betrokkenen een verzoek doen tot inzage in de wijze waarop wij diens persoonsgegevens gebruiken, wordt dit in beginsel toegewezen.

Verantwoording
Er dient altijd verantwoording te kunnen worden afgelegd over de wijze waarop met persoonsgegevens wordt omgegaan. Bij het gebruik van persoonsgegevens moet door medewerkers over bovenstaande uitgangspunten nagedacht zijn, proceseigenaren dienen hierin beslissingen te nemen, waar nodig met advies van de PO en/of de FG, en afwegingen hierbij moeten duidelijk gemaakt kunnen worden. Verantwoording naar het College vindt plaats door de FG door middel van de op te leveren producten die in hoofdstuk 7 worden omschreven.

5. Organisatie van beleid

Om het beleid op een goede manier te kunnen uitvoeren, maken wij de keuze om een aantal rollen en verantwoordelijkheden te beleggen op verschillende managementniveaus in onze gemeente. Hierbij wordt aangesloten bij onze netwerkorganisatie.

Functionaris Gegevensbescherming (FG)

Vanwege de verplichting hiertoe uit artikel 37 AVG hebben wij een FG aangesteld. De FG houdt intern toezicht op de naleving van de AVG en geeft hierover gevraagd en ongevraagd advies aan het College. De FG is daarnaast het aanspreekpunt voor de AP en is verantwoordelijk voor de afhandeling van klachten die direct aan de FG zijn gericht. De FG is niet aan te merken als verwerkingsverantwoordelijke en vervult een geheel onafhankelijke functie. De FG heeft hiertoe vrije toegang tot al onze systemen en processen en wij moeten medewerking verlenen wanneer de FG dit nodig heeft voor diens taakuitoefening.

Privacy Officer (PO)

De Raad heeft in de voorjaarsnota van 2018 besloten om een PO aan te stellen. Daar waar de FG een toezichthoudende en op hoog niveau adviserende rol heeft, heeft de PO een uitvoerende en een op laag niveau adviserende rol. Hierbij adviseert de PO medewerkers over het gebruik van persoonsgegevens binnen hun werkprocessen. Verder ziet de PO toe op een juist procedureverloop bij de uitvoering van de beleidsuitgangspunten en zorgt hierbij voor de nodige begeleiding. Ook zorgt de PO voor bewustwording aangaande het gebruik van persoonsgegevens. De PO is verder de beheerder van het privacybeleid, maar is niet aan te merken als verwerkingsverantwoordelijke. Tot slot heeft de PO een coördinerende rol bij het functioneren van het Privacyteam.

Chief Information Security Officer (CISO)

De CISO is onze adviseur voor informatiebeveiliging. Deze zoekt, waar nodig, de samenwerking op met de PO en de FG en zorgt dat de maatregelen die worden genomen en adviezen die worden gegeven in het kader van informatiebeveiliging aansluiten op het privacybeleid. Meer over de rol van de CISO is te lezen in het informatiebeveiligingsbeleid.

Privacyteam

Om een juiste link te kunnen leggen tussen de privacyregels en de werkprocessen en de vragen en behoeften van medewerkers hierbij, wordt gewerkt met een Privacyteam. Het Privacyteam bestaat uit medewerkers van alle teams, die fungeren als eerste aanspreekpunt voor de medewerkers in hun team bij vragen aangaande het gebruik van persoonsgegevens binnen hun werkzaamheden. Verder dient het Privacyteam als aanspreekpunt en adviseur voor de PO en de FG en als uitvoerder waar het gaat om implementatie van het privacybeleid en de AVG in de werkprocessen en de kaders die hierbij een rol spelen. Ook hebben leden van het Privacyteam een signaleringsfunctie voor zaken binnen hun team waarbij de PO en/of de FG betrokken zouden moeten worden.

Proceseigenaren

De proceseigenaar is verantwoordelijk voor een juiste uitvoering van de werkprocessen die hij of zij onder zich heeft. Hier hoort dus ook naleving van de privacyregels binnen deze werkprocessen bij.

De proceseigenaar dient ervoor te zorgen dat de bovenstaande uitgangspunten worden nageleefd en neemt hiertoe de nodige maatregelen. De proceseigenaar is bevoegd om besluiten te nemen over de wijze waarop binnen de werkprocessen met persoonsgegevens wordt omgegaan, maar dient hierover wel verantwoording af te kunnen leggen.

College van Burgemeester en Wethouders
Het College stelt het beleid vast en bevordert de beschikbaarheid van voldoende middelen om naleving van het beleid te kunnen realiseren. Het College is de verwerkingsverantwoordelijke voor alle verwerkingen van persoonsgegevens die op basis van dit beleid worden verricht en is in dat kader dus ook de eindverantwoordelijke voor een juiste naleving van de AVG en het privacybeleid.

6. Risico's en maatregelen

De uitgangspunten uit dit beleid zijn gebaseerd op de wettelijke vereisten vanuit de AVG. Wanneer deze niet worden nageleefd, kan dit tot gevolg hebben dat persoonsgegevens op onrechtmatige wijze worden gebruikt. Hierdoor kan de beschikbaarheid, integriteit en vertrouwelijkheid van de persoonsgegevens niet worden gegarandeerd. Dit kan grote gevolgen hebben voor betrokkenen. Denk hierbij aan de mogelijkheid tot identiteitsdiefstal en -fraude of schaamte wanneer bepaalde persoonsgegevens op straat komen te liggen. Ook kan het gebruik maken van bijvoorbeeld onjuiste, teveel of te weinig persoonsgegevens tot gevolg hebben dat verkeerde besluiten worden genomen, hetgeen serieuze consequenties voor inwoners kan hebben.

Wanneer persoonsgegevens op een verkeerde wijze worden gebruikt of keuzes hierbij niet goed kunnen worden verantwoord, kan dit ook grote gevolgen hebben voor ons. Wij kunnen hier door de AP namelijk op worden aangesproken en dit kan resulteren in hoge boetes en dus grote financiële consequenties hebben. Bovendien kan de negatieve publiciteit die hieraan vasthangt resulteren in imagoschade voor ons en hierdoor kan het vertrouwen van inwoners in ons een deuk oplopen.

De volgende maatregelen worden genomen om bovenstaande risico's zoveel mogelijk te beperken:

- Door de PO en CISO wordt regelmatig gefocust op bewustwording en informatievoorziening. Het doel hiervan is om medewerkers na te laten denken over hun omgang met persoonsgegevens en het belang van de naleving van het beleid extra te benadrukken.
- Medewerkers krijgen extra handvatten aangereikt waarmee zij zelf kunnen bepalen hoe zij binnen hun werkzaamheden de uitgangspunten op een juiste manier kunnen toepassen. Samen met het Privacyteam zal de PO hiertoe voor ieder team aparte richtlijnen opstellen, afgestemd op de specifieke wensen en behoeften van het desbetreffende team. Verder wordt gezorgd voor afdoende privacy-aanspreekpunten in de organisatie.
- Op risicovolle nieuwe gegevensverwerkingen worden risicoanalyses uitgevoerd in de vorm van gegevensbeschermingseffectbeoordelingen (DPIA's). Er worden vervolgens maatregelen genomen om de risico's die in kaart zijn gebracht zoveel mogelijk te beperken.
- De FG voert binnen ieder team de toezichthoudende taken uit aan de hand van de uitgangspunten uit dit beleid. Er wordt gerapporteerd en geadviseerd aan de teammanager en het College over maatregelen die genomen moeten worden om de AVG en het privacybeleid op een juiste wijze implementeren in de werkprocessen binnen deze teams.

- Privacy wordt meegenomen in de jaarlijkse ENSIA rapportage. Daarnaast vindt jaarlijks een verantwoording plaats omtrent algehele implementatie van het privacybeleid en de AVG in de organisatie door middel van een gemeentebrede privacy zelfscan. Aan de hand van deze beoordeling maakt de PO een uitvoeringsplan op voor het daaropvolgende jaar.

7. Producten privacy

Bij de uitvoering van dit privacybeleid worden de volgende producten opgeleverd. Per product is een verantwoordelijke aangegeven.

Product	**Termijn**	**Verantwoordelijke medewerker**	**Vaststelling of goedkeuring door**
Privacy zelfscan gemeentebreed	Jaarlijks	FG	Directieteam met kennisgeving College
Uitvoeringsplan n.a.v. privacy zelfscan	Jaarlijks	PO	Teammanager
Toezichts- en adviesrapporten incl. verbetermaatregelen	Continu	FG	Teammanager
DPIA incl. verbetermaatregelen per nieuwe risicovolle gegevensverwerking/proces	Alvorens de gegevensverwerking/het proces wordt uitgevoerd	Proceseigenaar	Teammanager
Privacybeleid	1x per 4 jaar, jaarlijkse actualisering	PO	College
Privacy richtlijnen per team	1x in 2019, actualisering wanneer nodig	PO en Privacyteam	Teammanager
Standaard DPIA-rapportagemodel	1x in 2019, actualisering wanneer nodig	PO	Teammanager
Herziene procedure rechten betrokkenen	1x in 2019, actualisering wanneer nodig	PO	Teammanager
Herziene procedure datalekken	1x in 2019, actualisering wanneer nodig	PO	Teammanager
Register van gegevensverwerkingen	1x in 2019, continue actualisering	Vaststelling: PO, Actualisering: proceseigenaren	Teammanager

8. Onderwerpspecifieke beleidskeuzes

Naast de algemene uitgangspunten is, gezien de gevoelige aard, besloten om voor de volgende processen en de gegevensverwerkingen die daarbij horen aparte uitgangspunten vast te stellen.

Integraal werken

Wij hebben als beleid om integraal te werken om zo op maat afgestemde dienstverlening aan inwoners en bedrijven te kunnen bieden. Er zitten echter grenzen aan hetgeen in het kader van

integrale gegevensverwerking is toegestaan. Tijdens mondelinge gesprekken met inwoners mogen persoonsgegevens integraal worden opgevraagd. Verdergaande integrale verwerking van persoonsgegevens (bijvoorbeeld het opslaan of het verwerken in een gespreksverslag) mag vervolgens alleen wanneer dit noodzakelijk is om te kunnen voorzien in een specifieke hulpvraag die voorligt of voor de uitvoering van een wettelijke taak.

Cameratoezicht
Binnen onze gemeente wordt gebruik gemaakt van cameratoezicht wanner dit noodzakelijk is om de veiligheid te kunnen waarborgen en in dat kader toezicht te houden op openbare plaatsen. Als sprake is van een verhoogd veiligheidsrisico in een bepaald gebied, is inzet van camera's mogelijk op projectmatige basis. Op verzoek van ondernemers worden camera's op bedrijventerreinen tijdelijk toegestaan als de veiligheid daarmee is gediend.

Big data verwerkingen
Wij kunnen gebruik maken van Big data verwerkingen met als doel dat dit de gemeentelijke dienstverlening ten goede komt, waarbij enkel gebruik wordt gemaakt van pseudonimiseerde of geanonimiseerde persoonsgegevens.

Profilering
Wij kunnen gebruik maken van profilering wanneer dit noodzakelijk voor de uitvoering van een overeenkomst tussen ons en de betrokkene, dit toegestaan is door Nederlands of Europees recht of wanneer hiervoor toestemming van de betrokkene is verkregen.

Begrippenlijst

- Anonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld.
- Betrokkenen: geïdentificeerde of identificeerbare natuurlijke personen. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. In het kader van dit privacybeleid zijn dit inwoners en medewerkers.
- Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Dit betekent concreet dat persoonsgegevens mogelijk permanent worden verwijderd of mogelijk in verkeerde handen vallen.
- Data Protection Impact Assessment (DPIA): een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Dit wordt ook wel een gegevensbeschermingeffectbeoordeling genoemd.
- Nieuwe of gewijzigde werkprocessen: denk hierbij niet alleen aan een ander stappenplan aan de hand waarvan het werkproces wordt doorlopen, maar ook aan nieuwe samenwerkingen/uitbestedingen of het gebruik van nieuwe systemen/applicaties.
- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Bedrijfsgegevens vallen buiten het toepassingsbereik van de AVG.
- Profilering: een geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen.
- Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
- Rechten betrokkenen: behoudens uitzonderingen, kunnen betrokkenen de volgende rechten inroepen in het kader van de hen aangaande persoonsgegevens:
    - Dataportabiliteit: het recht om persoonsgegevens overgedragen te krijgen naar een andere partij.
    - Vergetelheid: het recht om 'vergeten' te worden.
    - Inzage: het recht om de persoonsgegevens die de gemeente verwerkt in te zien en kennis te nemen van wat met de persoonsgegevens gebeurt.
    - Rectificatie en aanvulling: het recht om de persoonsgegevens die de gemeente verwerkt te wijzigen.

    - Beperking van de verwerking: het recht om minder gegevens te laten verwerken.
    - Niet onderworpen worden aan geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten.
    - Bezwaar: het recht om bezwaar te maken tegen de gegevensverwerking.
- Rechtsgrondslag: basis die verwerking van persoonsgegevens rechtvaardigt. Hierbij bestaan, op grond van artikel 6 van de AVG, de volgende mogelijkheden: toestemming van de betrokkene, een overeenkomst tussen de betrokkene en de gemeente, een wettelijke verplichting van de gemeente, een vitaal belang van de betrokkene, werkzaamheden van de gemeente in het kader van algemeen belang of openbaar gezag of een gerechtvaardigd belang van de gemeente.
- Verwerking: 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. Meer concreet houdt dit in alle handelingen die worden verricht met persoonsgegevens.
- Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit privacybeleid is dit het College.