Gemeente Rucphen

GEMEENTEBLAD

Officiële uitgave van de gemeente Rucphen

Nr. 313344

17 juli

2023

Privacybeleid 2023-2026 Gemeente Rucphen

Artikel 1 Inleiding

1.1. Algemeen

Binnen de gemeente Rucphen wordt gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat.
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 wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).
Dit beleid heeft betrekking op de gemeente Rucphen als bestuursorgaan en als werkgever.
In dit beleid wordt beschreven hoe de gemeente invulling geeft aan de privacy uitgangspunten en de verplichtingen die de AVG met zich meebrengt. Het beleid is algemeen beleid op hoofdlijnen. Dat betekent dat de uitwerking van het beleid plaatsvindt in onderliggende documenten zoals de privacygovernance, de privacyverklaring, procedurebeschrijvingen, protocollen en werkinstructies.

1.2. Kernwaarden

De gemeente Rucphen vindt het belangrijk dat de gegevens van de burgers goed beschermd worden. Daartoe hanteren we onderstaande kernwaarden.

1. De mens staat centraal
   Onze organisatievisie is “Samenwerken aan resultaat en mens”. We zoeken steeds meer contact met onze inwoners om samen met hen te zoeken naar ‘de beste oplossing’. We willen niet langer denken vanuit onze systemen en regels, maar zoeken samen naar mogelijkheden en ruimte. Hierbij zorgen wij ervoor dat wij mens met respect behandelen waarbij privacy hoog in het vaandel staat.

2. Een heldere belangenafweging
   De uitvoering van onze wettelijke taken, optimale dienstverlening en privacybescherming betekenen dat wij steeds zoeken naar een goed evenwicht. Bij het zoeken naar ‘de beste oplossing” voor onze inwoners wordt zorgvuldig gekeken naar het belang van het individu tegenover het algemeen belang, het wettelijke kader, een correcte risicoafweging en ons moreel kompas. Wij geloven dat een goede privacybescherming, dienstverlening en werkbaarheid samengaan.

3. Digitale veiligheid
   Bij digitaal werken is digitale veiligheid en bescherming van persoonsgegevens belangrijk. Burgers moeten er op kunnen vertrouwen dat hun persoonsgegevens veilig zijn bij ons. Het privacybeleid steunt dan ook op de uitgangspunten die verwoord zijn in het Informatieveiligheidsbeleid. Ondanks dat er voornamelijk digitaal gewerkt wordt, geldt veiligheid en bescherming uiteraard ook voor analoge persoonsgegevens, fysiek op papier.

4. Eenmalige vastlegging, meervoudig gebruik
   Wij willen niet steeds opnieuw persoonsgegevens vragen die bij ons al bekend zijn. Wij vragen gegevens alleen met een wettelijke grondslag. Bij onze rol als overheid en werkgever horen de grondslagen ‘wettelijke verplichting’ en ‘taak van algemeen belang en/of openbaar gezag’. Omdat er tussen burger/werknemer en overheid/werkgever een afhankelijkheidsrelatie ervaren kan worden, verwerken wij bij voorkeur geen persoonsgegevens op basis van de grondslag toestemming.

5. Openheid
   Wij vinden het waardevol dat onze burgers vertrouwen hebben in ons als gemeente. Daarbij speelt openheid een belangrijke rol. Dit betekent dat wij burgers op passende manieren informeren

over hun privacyrechten. Hiervoor gebruiken wij verschillende methoden. Daarnaast informeren wij burgers door een algemene privacyverklaring[1] openbaar te maken.

1.3. Ambities

De afgelopen jaren heeft de gemeente Rucphen al veel bereikt om te voldoen aan de privacy wet- en regelgeving. Zo is er een projectgroep Betrouwbaar Rucphen sinds medio 2020 aan de slag die werkt aan de bewustwording, waaronder ook op het gebied van privacy. Ook is een stap in het volwassenheidsniveau gemaakt door sinds juni 2021 te werken met privacy ambassadeurs op de afdelingen. Het volwassenheidsniveau wordt binnen onze gemeente bepaald aan de hand van een VNG-toetsingsinstrument[2]. Onze doelstelling is om volwassenheidsniveau 3 te behalen en de komende jaren te streven om door te groeien naar 4. Dit privacybeleid vormt de basis voor de gemeente Rucphen om deze ambitie waar te maken.

1.4. Scope van dit beleid

Het privacybeleid omvat de gehele datastroom van persoonsgegevens binnen de gemeente. Van het genereren of verzamelen van persoonsgegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging van persoonsgegevens.
Het beleid strekt zich ook uit over de verwerkingen van politiegegevens op grond van de Wet Politiegegevens (WPG). Binnen onze gemeente zijn buitengewoon opsporingsambtenaren (boa's) werkzaam. Persoonsgegevens die door boa's in het kader van de opsporing van strafbare feiten worden verwerkt vallen niet onder de AVG, maar onder de Wpg. Persoonsgegevens die onder deze wet vallen worden politiegegevens genoemd. Daar, waar in dit beleid wordt gesproken over de verwerking van persoonsgegevens, worden alle verwerkingen, dus zowel verwerkingen onder de AVG als de Wpg, bedoeld.
Wanneer we persoonsgegevens delen met onze (keten)partners of leveranciers bij uitbesteding van taken of bij samenwerking gelden dezelfde uitgangspunten die opgenomen zijn in dit privacybeleid. Hiervoor maken wij contractuele afspraken ten aanzien van de verwerking van persoonsgegevens die we ook kunnen toetsen bij de uitvoering van de werkzaamheden.
Dit betekent dat het beleid van toepassing is op:

* de gehele gemeentelijke organisatie en de taakuitoefening van bestuurders en medewerkers;
* alle processen waarbinnen persoonsgegevens worden verwerkt;
* informatiesystemen die de gemeente gebruikt waarin persoonsgegevens worden verwerkt;
* alle objecten, ruimten en apparaten die door medewerkers worden gebruikt waar(op) persoonsgegevens worden verwerkt;
* onze (keten)partners, leveranciers waar we persoonsgegevens mee delen en die deze persoonsgegevens voor de gemeente verwerken.

Voor bepaalde domeinen kan het nodig zijn om specifiek privacybeleid vast te stellen. Zo is er bijvoorbeeld privacybeleid sociaal domein.
Naast dit privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

2. Privacy uitgangspunten

De gemeente Rucphen hanteert de uitgangspunten *Rechtmatigheid*, *Behoorlijkheid* en *Transparantie* om invulling te geven aan alle uitgangspunten die de AVG stelt. Hieronder worden deze punten kort omschreven en de wijze waarop wij concreet invulling hieraan geven binnen onze organisatie.

2.1. Rechtmatigheid

Voor een verwerking van persoonsgegevens hebben wij altijd een geldige grondslag. Deze grondslag stellen wij vast voorafgaand aan de eerste verwerking van persoonsgegevens. De rechtmatigheid van de grondslag wordt getoetst.
Als wij persoonsgegevens vaker gebruiken, intern of extern verstrekken, delen of uitwisselen dan is het doel daarvan verenigbaar met de oorspronkelijke verzameldoeleinden (doelbinding). Als blijkt dat het niet verenigbaar is, dan wordt gekeken naar een rechtmatige grondslag.
Wij leggen alleen persoonsgegevens vast als dit noodzakelijk is voor het specifieke doel van de verwerking. Diverse gemeentelijke taken (algemeen belang/openbaar gezag) vereisen het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd. In het verwerkingsregister wordt per

verwerking concreet gemaakt op basis van welke grondslag en met welk doel de verwerking van persoonsgegevens gerechtvaardigd is.

2.2. Behoorlijkheid

Wij vragen slechts díe persoonsgegevens die noodzakelijk zijn om het beoogde doel te bereiken (proportionaliteit). Daarbij gebruiken wij altijd de methode die de minste inbreuk maakt op de persoonlijke levenssfeer van de betrokkenen (subsidiariteit).
Wij richten onze systemen en processen zodanig in dat niet te veel persoonsgegevens worden gevraagd.
Wij hanteren het beginsel van 'éénmalige vastlegging, meervoudig gebruik': persoonsgegevens die bekend zijn worden in principe niet opnieuw gevraagd. Wij maken zo veel mogelijk gebruik van brongegevens zoals die zijn opgenomen in het stelsel van basisregistraties. Dit is slechts mogelijk als er een wettelijke grondslag en een verenigbaar doel is.
Persoonsgegevens worden niet langer bewaard dan noodzakelijk is.
Alleen functionarissen (ambtenaren, externen, leveranciers, convenantpartners), waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. Verder hebben wij een autorisatiebeleid zodat slechts functionarissen toegang hebben tot de persoonsgegevens die hier ook echt een functioneel doel voor hebben.
Met externen, samenwerkingspartners, verwerkers en leveranciers maken wij schriftelijke privacyafspraken, vastgelegd in overeenkomsten en convenanten.
Persoonsgegevens worden goed beveiligd opgeslagen, zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking.

2.3. Transparantie

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente Rucphen heeft verzameld en waarvoor deze worden gebruikt. Dit gebeurt onder meer door onze privacyverklaring op de website.
Verder wordt per nieuwe verwerking van persoonsgegevens bekeken hoe de betrokkenen op een passende wijze geïnformeerd kunnen worden.
Om recht te doen aan verzoeken van betrokkenen hebben wij de 'procedure rechten van betrokkenen AVG en Wpg[3] vastgesteld. Hierin is beschreven hoe verzoeken van betrokkenen door ons worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft.

3. Verplichtingen AVG en Wpg

Hieronder worden deze verplichtingen omschreven inclusief de feitelijk uitwerking daarvan binnen onze organisatie. Dit geeft tevens aan hoe wij invulling geven aan de uitgangspunten in het vorige hoofdstuk.

3.1. Het verwerkingenregister

Binnen de gemeente zijn er veel processen waarbij sprake is van het verwerken van persoonsgegevens en politiegegevens. De gemeente heeft van deze verwerkingen een verwerkingenregister opgesteld.
Het MT heeft de "Procedure Beheer Verwerkingenregister AVG en Wpg[4]" vastgesteld. In die procedure is beschreven wie verantwoordelijk is voor het verwerkingenregister, wat in het register moet worden opgenomen en hoe dit bijgehouden moet worden.

3.2. Data Protection Impact Assessment (DPIA)

Als een verwerking mogelijk een hoog risico inhoudt voor de privacy van de betrokkene, dan moet de gemeente de privacy risico's van die verwerking van persoonsgegevens in beeld brengen. De gemeente voert in dat geval een gegevenseffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd).
Een DPIA kun je zien als een inhoudelijk gesprek tussen de proceseigenaar, de procesverantwoordelijke, de CISO[5] en de privacy coördinator over het werkproces en de applicatie die daar eventueel voor wordt gebruikt. In dit DPIA gesprek worden de risico's bepaald die er zijn en worden maatregelen benoemd om de risico's te verkleinen. Doel is om te bepalen of de maatregelen voldoende en de risico die overblijven aanvaardbaar zijn. Dit alles wordt vastgelegd in een rapportage.
Hoe, door wie en wanneer een DPIA uitgevoerd wordt, is beschreven in de "Procedure Uitvoeren Data Protection Impact Assessment (DPIA)[6]". Dit zodat duidelijk is welke stappen doorlopen moeten worden om te voldoen aan de AVG en Wpg.

3.3. Privacy by design & Privacy by default

Wij hanteren de principes ‘Privacy by Design’ en ‘Privacy by Default’ op verwerkingen van persoons- én politiegegevens.
Privacy by design houdt in dat wij er bij het ontwerpen van producten en diensten voor zorgen dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of de bouw van een systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische beveiligingsmaatregelen. Privacy wordt aan het begin van projecten en inkoopprocessen meegenomen.
Privacy by default houdt in dat wij werkprocessen inrichten en de standaardinstellingen van een programma instellen op de meest privacy vriendelijke manier. Zonder daarbij de functionaliteit, gebruiksvriendelijkheid, werkbaarheid, effectiviteit en efficiency uit het oog te verliezen. In de risicoanalyse (zoals beschreven in paragraaf 3.5) worden de voor privacy by design/default noodzakelijke aspecten meegenomen in de voorgenomen verwerking. Op deze manier borgen wij dat nieuwe verwerkingen volgens de normen van Privacy by design/default worden ingericht.
Als passende maatregelen nog niet worden afgedwongen in systemen zorgen wij voor aanvullende organisatorische en/of technische maatregelen om dit alsnog te borgen.

3.4. Datalekken

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico op de privacy van betrokkenen, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms moeten de betrokkenen over het datalek geïnformeerd worden.
Wij registreren datalekken, zetten de bevindingen om in verbeterpunten en zien toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het‘ Protocol Melden Beveiligingsincidenten/ Datalekken’[7].

3.5. Rechten van Betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten ingevolge de AVG en Wpg uit te oefenen. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen AVG en Wpg[8].

3.6. Functionaris Gegevensbescherming (FG)

De gemeente Rucphen is een overheidsinstantie. Het is in dit geval een wettelijke verplichting om een FG aan te stellen. De gemeente Rucphen heeft een FG aangewezen voor zowel de AVG als de Wpg.
De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit van zijn werkzaamheden, bevindingen en aanbevelingen.

3.7. Beveiliging

Op grond van de AVG en de Wpg dienen organisaties passende technische en organisatorische maatregelen te nemen om de persoonsgegevens die zij verwerkt, te beveiligen.
De gemeente Rucphen heeft strategisch en tactisch informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling wordt gegeven aan de passende maatregelen ter beveiliging van persoonsgegevens. De gemeente Rucphen conformeert zich aan de Baseline Informatiebeveiliging Overheid[9]. Dit normenkader wordt door ons actief toegepast op alle verwerkingen van persoonsgegevens.
Wij hebben een Chief Information Security Officer (CISO) aangesteld die de passende maatregelen implementeert en een veilig gebruik van persoonsgegevens bevordert.

3.8. Gegevens delen met derden

Wanneer er sprake is van structurele of gevoelige gegevensuitwisseling met derde partijen, maken wij afspraken over de gegevensuitwisseling. Deze afspraken voldoen tenminste aan de AVG en Wpg en worden vastgelegd in een onderlinge regeling, een samenwerkingsovereenkomst (convenant), een gegevensuitwisselingsovereenkomst of een verwerkersovereenkomst. De gemeente Rucphen gebruikt landelijke standaarden en richtlijnen om de contractuele verplichtingen te regelen met derden.[10]
Bij het intern en extern delen en uitwisselen van persoonsgegevens zorgen wij dat er een aantoonbare binding is met het oorspronkelijke doel.
De gemeente Rucphen geeft in principe geen persoonsgegevens door aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar

rechtmatig is.
In de volgende gevallen mogen persoonsgegevens doorgegeven worden aan een derde land buiten de EER:
* Met een adequaatheidsbesluit;
* Met passende waarborgen met een modelcontract (Standard Contractual Clauses);
* Met binding corporate rules (BCR);
* Met specifieke uitzonderingen, zoals bijvoorbeeld privacy risico's die acceptabel zijn.

3.9 Politiegegevens ter beschikking stellen en verstrekken

In de Wpg wordt onderscheid gemaakt tussen het delen van gegevens binnen en buiten het Wpg domein.

Binnen het Wpg domein – Ter beschikking stellen
Indien er door onze Boa's binnen het Wpg domein gegevens worden gedeeld is er sprake van ter beschikking van politiegegevens. Bij het ter beschikkingstellen is sprake van het zogenaamde "free flow of information[11]. Ambtenaren die aangewezen zijn als opsporingsambtenaar bij de politie, de Koninklijke Marechaussee, Bijzondere Opsporingsdiensten of Boa's mogen onderling politiegegevens delen.
Hierbij geldt altijd het 'need-to-know principe': de ontvanger moet de gegevens nodig hebben voor zijn taak. Buiten deze vier aangewezen groepen personen mogen er geen politiegegevens worden verwerkt.

Buiten het Wpg domein – Verstrekken
In de Wpg is vastgelegd aan welke partijen buiten het Wpg-domein een Boa gegevens mag verstrekken. In dat geval gaan de persoonsgegevens van het Wpg regime naar het Avg regime. Voor elke verstrekking geldt dat deze moet worden geadministreerd. Als een betrokkene om inzage vraagt, moet hij namelijk kunnen zien met wie zijn gegevens zijn gedeeld.
In de Verstrekkingenwijzer voor boa's[12] is uitgewerkt aan wie verstrekt mag worden en wat de voorwaarden zijn. Deze wijzer geldt voor alle boa's in Nederland.

4. Risico's

De gemeente Rucphen hanteert een beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. Dit kader geeft invulling aan het AVG normenkader voor het duiden van privacyrisico's en de daarbij behorende beheersmaatregelen.
Het is belangrijk om dit inzicht te hebben. Dit privacybeleid, in combinatie met het informatiebeveiligingsbeleid, heeft als doel de privacyrisico's te verkleinen.

5. Taken & verantwoordelijken

Het college is verantwoordelijk voor het naleven van de privacy wet- en regelgeving en de kaders voor het verantwoord omgaan met persoonsgegevens. De gemeente heeft de verantwoordingsplicht om te kunnen aantonen dat deze uitgangspunten en kaders worden nageleefd. Elke medewerker binnen onze organisatie is in diverse mate verantwoordelijk voor de juiste naleving en implementatie van dit privacybeleid. De concrete interne taakverdeling om dit te borgen is vastgelegd in de Privacy Governance[13].

6. Bewustwording

Een hoge mate van bewustwording bij alle medewerkers is van essentieel belang om dit privacybeleid goed uit te voeren. De gemeente Rucphen streeft een adequaat niveau van bewustwording na als het gaat om privacy en informatiebeveiliging. Er wordt continue aandacht geschonken aan bewustwording.

7. Verantwoording

Het college is het bestuursorgaan dat de passende technische en organisatorische maatregelen[14] treft voor alle verwerkingsverantwoordelijken, waaronder ook voor de gemeenteraad en de burgemeester.
De wijze waarop de maatregelen worden getroffen, om te voldoen aan de verplichtingen van de AVG en Wpg (hoofdstuk 3 van dit beleid) worden uitgeschreven in procedurebeschrijvingen, protocollen en werkinstructies.
Het college zal via de Planning en Control Cyclus (P&C Cyclus) verantwoording afleggen over het

naleven van de AVG en Wpg aan de gemeenteraad. Dit zodat de gemeenteraad zijn controlerende taak goed uit kan oefenen.
De FG brengt jaarlijks verslag uit aan het college over de ontwikkelingen en aandachtspunten bij de omgang met persoonsgegevens. Dit jaarverslag van de FG is onderdeel van de P&C Cyclus.

8. Uitwerking en evaluatie

De verantwoordelijkheid om het beleid uit te werken in specifiek uitvoeringsbeleid, procedurebeschrijvingen, protocollen en werkinstructies ligt bij het lijnmanagement. De privacy Coördinator heeft hier een adviserende en, zo nodig, een ondersteunende rol.
Eens in de drie jaar, of eerder indien daar aanleiding toe is, wordt dit privacybeleid geëvalueerd en aangepast.
Specifiek uitvoeringsbeleid, procedurebeschrijvingen, protocollen en werkinstructies worden jaarlijks, op verzoek en in overleg met de privacy Coördinator, door het lijnmanagement geëvalueerd.

9. Inwerkingtreding en citeertitel

Het college heeft het privacybeleid op 27 juni 2023 vastgesteld en treedt een dag na bekendmaking in werking. Dit beleid wordt aangehaald als "Privacybeleid gemeente Rucphen 2023 – 2026
Het Privacybeleid gemeente Rucphen, de Privacybelofte en het Privacyreglement vastgesteld op 29 mei 2018 worden per die datum ingetrokken.

Besloten in de vergadering van burgemeester en wethouders d.d. 27 juni 2023

de secretaris,	de burgemeester,
S. Michielse	mr. M. van der Meer Mohr

[1] *Privacyverklaring website*
[2] *AVG-Borgingsproduct 2.0*
[3] *Procedure rechten van betrokkenen AVG en Wpg d.d. 12 december 2022*
[4] *Procedure beheer verwerkingenregister AVG en Wpg, d.d. 12 december 2022*
[5] *Chief Information Security Officer*
[6] *Procedure Uitvoeren Data Protection Impact Analyse (DPIA) d.d. 12 december 2022*
[7] *Protocol Melden Beveiligingsincidenten/Datalekken d.d. 20 juni 2022. Dit protocol is ook van toepassing is op politiegegevens.*
[8] *Procedure Rechten van betrokkenen AVG en Wpg d.d. 12 december 2022*
[9] *https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/*
[10] *Wij hanteren het landelijk toegepaste en bindende modellen van de VNG/IBD*
[11] *Ook wel het ter beschikking stellen ingevolge artikel 15 Wpg.*
[12] *https://www.natuurnetwerk.info/BRS-Verstrekkingenwijzer/?v=2*
[13] *Beschrijving taken en rollen Privacy Coördinator – Privacy Ambassadeur - Afdelingsmanager – Chief Information Security Officer – Functionaris Gegevensbescherming d.d. 12 december 2022*
[14] *Artikel 24 AVG en artikel 4a Wpg*