gemeente Rhenen

GEMEENTEBLAD

Officiële uitgave van de gemeente Rhenen

Nr. 514469

26 november 2025

Gemeente Rhenen - Gegevensbeschermingsbeleid 2025

Het college besluit:
- het Gegevensbeschermingsbeleid 2025 vast te stellen;
- het Gegevensbeschermingsbeleid (voorheen Privacybeleid 2020) in te trekken.

I Inleiding

Doel van het beleid

Dit document geeft weer hoe de gemeente invulling geeft aan een verantwoorde omgang met persoonsgegevens binnen de kaders van de relevante wetgeving.
Dit beleid beschrijft de uitgangspunten om de gevolgen van incidenten en onzorgvuldige verwerking van persoonsgegevens binnen administratieve processen te beperken tot een acceptabel niveau.

Het beleid is van toepassing op iedereen die onder verantwoordelijkheid van de gemeente persoonsgegevens verwerkt. Dit betreft zowel vaste medewerkers als ingehuurde krachten en externe partijen die werkzaamheden uitvoeren in opdracht van de gemeente. beleid is gericht op medewerkers, ingehuurde medewerkers en externen, die in opdracht van de gemeente persoonsgegevens verwerken.

Gegevensbescherming uitgelegd

Gegevensbescherming draait om de bescherming van de grondrechten van betrokkenen tegen de keerzijden van de verwerking van hun gegevens. De gemeente heeft gegevens nodig om haar gemeentelijke taken uit te kunnen voeren. Betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met persoonsgegevens omgaat, en dat de gemeente voorkomt dat er een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer. Dit doet zij door het treffen van passende technische en organisatorische maatregelen om de risico's inzichtelijk te maken en deze vervolgens voor de betrokkenen tot een geaccepteerd niveau te beperken. Vanuit gegevensbescherming bezien vormt informatiebeveiliging daarbij een hygiënefactor.
Voor zover dit nog niet bij wet voorzien is, weegt de gemeente hierbij de belangen van het individu af tegen dat van anderen. Dit kan betekenen dat het individueel belang soms moet wijken voor het algemene belang, of andersom: dat we als gemeente besluiten dat een verwerking van persoonsgegevens onwenselijk is omwille van de potentiële impact op het individu.

Wettelijke kaders

• De Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG).
De AVG stelt kaders voor een verantwoorde omgang met persoonsgegevens. Deze kaders bestaan deels uit open normen, zoals behoorlijkheid en transparantie of passende waarborgen, die nadere invulling behoeven.
In artikel 5 staan de principes van de AVG:

1. Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.
2. Het waarom van de verwerking van de persoonsgegevens moet uitdrukkelijk omschreven zijn èn er moet sprake zijn van een gerechtvaardigd doeleinde (doelbinding). Verdere verwerking van deze gegevens moet verenigbaar zijn met het oorspronkelijke doeleinde.
3. Persoonsgegevens moeten voldoende zijn, maar ook niet meer dan nodig. Te veel aangereikte informatie mag niet worden meegenomen in de verwerking. (dataminimalisatie).
4. Persoonsgegevens moeten juist zijn, en zonodig worden geactualiseerd (juistheid)
5. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is. (Opslagbeperking) In bepaalde gevallen mogen deze gegevens wel langer bewaard worden, bijvoorbeeld voor wetenschappelijk onderzoek. Dan moeten de gegevens worden aangepast, zodat niet meer duidelijk is van wie deze gegevens waren.
6. Passende beveiliging is nodig, zodat de persoonsgegevens ongeoorloofde en onrechtmatige verwerking niet plaats kan vinden. Ook bescherming tegen onopzettelijk verlies, vernietiging en beschadiging is nodig (Veiligheid).

• De Wet Politiegegevens (Wpg) en het Besluit politiegegevens Boa's (Bpg Boa).
De Wpg stelt eigen eisen aan de verwerking van persoonsgegevens
Als boa-werkgever heeft de gemeente niet alleen te maken met de AVG, maar ook met de Wpg. Op het moment dat een BOA toezicht houdt, valt dit onder de AVG, maar wanneer er een proces -verbaal wordt opgesteld, dan valt dit onder de Wpg. De persoonsgegevens worden daarmee politiegegevens.
Op basis van de Wpg mogen en moeten we soms politiegegevens doorgeven aan andere boa’s of medewerkers van andere opsporingsdiensten zoals de politie. Zij hebben deze gegevens nodig voor

de uitvoering van hun taken. Ook aan andere instanties, zoals bijvoorbeeld het Openbaar Ministerie, kunnen politiegegevens worden doorgegeven.
Onder de AVG heeft de gemeente een verantwoordingsplicht en moet kunnen aantonen dat zij voldoet aan de zes principes van de AVG.
Voor de Wpg activiteiten moet de gemeente registers bijhouden en moet de gemeente audits laten uitvoeren.

Visie
De kernwaarden van gemeente Rhenen zijn 'Flexibel, vertrouwen, samenwerken & verantwoordelijkheid'. We kennen en nemen onze verantwoordelijkheid, mogen vertrouwen op de deskundigheid van de medewerkers van de gemeente, we streven samenwerking na en we stellen ons flexibel op.

De gemeente Rhenen werkt 'vanuit de bedoeling'. Dit betekent werken met de blik naar de samenleving waarbij de inwoner centraal staat. Dit betekent voor gegevensbescherming dat we zoeken naar mogelijkheden binnen de gestelde kaders. De AVG vereist risico gebaseerd werken, wat inhoudt dat ook bij het verkennen van mogelijkheden de risico's vooraf in kaart worden gebracht en beoordeeld.

Ambitie
De gemeente Rhenen is een kleine gemeente, die heeft uitgesproken een slimme volger te willen zijn. Dat houdt in dat het niet binnen de ambitie van de gemeente Rhenen ligt om koploper te worden en een landelijke projectaanjager te zijn.
Gemeente Rhenen wil voldoen aan de geldende wet- en regelgeving, met daaraan gekoppeld een volwassenheidsniveau. Deze ambities zijn nader uitgewerkt in het implementatieplan van het Integraal Management Team.

Reikwijdte
Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens van alle betrokkenen die geheel of gedeeltelijk geautomatiseerd worden uitgevoerd. Het geldt voor de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente.

Beheer van dit document
Dit document is in beheer van de Privacy Officer en is het product van een samenwerking tussen portefeuillehouder, de Functionaris Gegevensbescherming en de Raad.
Een gegevensbeschermingsbeleid heeft geen vaste wettelijke geldigheidsduur volgens de AVG, maar het moet actueel en passend blijven bij de gegevensverwerkingen binnen je organisatie. Veel organisaties kiezen ervoor om het beleid minimaal één keer per twee jaar te evalueren en te actualiseren. Dit helpt om compliant te blijven en toont aan dat je de verantwoordingsplicht serieus neemt.
Het beleid wordt vastgesteld door het College van Burgemeester en Wethouders.

Implementatieplan
De concrete stappen die genomen moeten worden ten aanzien van de gegevensbescherming, staan beschreven in het implementatieplan. Dit is een levend document dat wordt gevoed vanuit diverse bronnen zoals: rekenkameronderzoek, het toezichtsplan en jaarverslag van de Functionaris Gegevensbescherming en ook het gegevensbeschermingsbeleid. Het eigenaarschap van het meerjarig implementatieplan ligt bij het Integraal Management Team.

Organisatie

De verantwoordelijkheden en rollen sluiten aan bij het Three Lines of Defence-model. In dit model is het lijnmanagement als eerste lijn verantwoordelijk voor het realiseren van gegevensbescherming binnen de eigen processen. De tweede lijn (Privacy Officer) ondersteunt en coördineert. In de derde lijn wordt het geheel door een (interne) auditor en/of de Functionaris voor de Gegevensbescherming van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Verantwoordelijkheden
College van Burgemeester en Wethouders.
Het College van Burgemeester en Wethouders is verwerkingsverantwoordelijke onder de AVG. Zij zijn bestuurlijk verantwoordelijk voor het gegevensbeschermingsbeleid. Binnen het college is een portefeuillehouder aangewezen.
De Raad.
De Raad wordt voor een aantal taken als gemeentelijk overheidsorgaan onder de AVG als verwerkingsverantwoordelijke aangemerkt. Daarnaast heeft de Raad een controlerende functie ten opzichte van het college voor de naleving van de AVG en stellen zij budget beschikbaar.

Eerstelijns rollen

Managers

De gemeente Rhenen heeft een drietal managers die samen met de gemeentesecretaris het Integraal Management Team (IMT) vormen. Het IMT buigt zich over een scala aan onderwerpen, neemt besluiten en stelt beleid dat de ambtelijke organisatie aangaat vast.
De managers zijn verantwoordelijk voor de teams die aan hen zijn toebedeeld.

Proceseigenaar

Voor elk proces moet er een verantwoordelijke medewerker zijn aangewezen (proceseigenaar) en een eindverantwoordelijke (manager). Hiermee wordt onderscheid gemaakt tussen verantwoordelijkheid in uitvoering (responsible) en aansprakelijkheid (accountable). Samen met diens manager is de proceseigenaar verantwoordelijk voor het ordentelijk verlopen van een proces. De proceseigenaar is verantwoordelijk voor de gegevensbescherming binnen de eigen processen en functioneert voor deze processen als contactpunt voor de 2e-lijnsondersteuning.

Teams

De gemeente Rhenen werkt met zelfsturende teams. Een proces is ondergebracht bij een team en kan door meerdere medewerkers worden uitgevoerd. Een proces heeft echter maar één proceseigenaar.

Tweedelijns rollen

Privacy Officer (PO)

De Privacy Officer ondersteunt de organisatie bij de implementatie van de gegevensbescherming. De PO is aanspreekpunt binnen de organisatie voor vragen op het gebied van gegevensbescherming. De PO werkt vanuit een implementatieplan waarin de accenten en prioriteiten voor de komende periode zijn vastgelegd.

Bevoegd functionaris (WPG)

De bevoegd functionaris Wpg heeft een belangrijke rol in het begeleiden van artikel 9 verwerkingen. Dit betreft opsporingsonderzoek met een verregaande inbreuk op de privacy van de betrokkene. Zoals het vastleggen van het doel van de verwerking, het bepalen van toegang en het verstrekken van politiegegevens.

Wpg -coördinator

De Wpg-Coördinator voert de regie op de uitvoering van de verplichte jaarlijkse interne- en vierjaarlijks externe audit op de implementatie van de Wet Politiegegevens en ondersteunt de organisatie bij de realisatie van de daaruit voortvloeiende verbetermaatregelen.

Derdelijns rollen

Functionaris voor de Gegevensbescherming (FG)

De FG is de AVG-autoriteit van de organisatie. De FG helpt de organisatie om het volwassenheidsniveau van de gegevensbescherming op het niveau te krijgen en te houden waar in de AVG van wordt uitgegaan. De FG toetst zowel structureel en incidenteel op naleving van de AVG, gerelateerde wetgeving zoals de Wpg en interne beleidsafspraken, en treedt op als adviseur bij gegevensbeschermingsvraagstukken. De FG behartigt de belangen van betrokkenen en treedt als ombudsman op in het geval van klachten. De FG is onafhankelijk en rapporteert aan het College van burgemeester & Wethouders en de Raad. Aan het begin van het kalenderjaar legt de FG in een Toezichtsplan de aandachtspunten van diens toezicht voor het komende jaar vast. Aan het eind van het jaar beoordeelt de FG in diens Jaarverslag de voortgang van de implementatie van gegevensbescherming door de gemeente.

Overlegstructuren

Managers / IMT

Vanuit gegevensbescherming vinden gesprekken met de afzonderlijke managers plaats over de gegevensbescherming binnen het eigen domein, alsook gesprekken met het IMT als geheel, onder andere over het implementatieplan en de tot stand gekomen vorderingen.

FG-CISO-PO

Tijdens het wekelijks overleg tussen de FG, de Ciso en de PO worden actuele casussen besproken op het gebied van gegevensbescherming en informatiebeveiliging.

Portefeuillehouder

Vanuit gegevensbescherming wordt deelgenomen aan de overleggen met de portefeuillehouder. Dit contactmoment kan onder andere gebruikt worden voor het op strategisch niveau spreken van de implementatie van de gegevensbeschermingsactiviteiten en over ontwikkelingen op nationaal en internationaal vlak.

Raad

Er is tweemaal per jaar (maart en september) een commissievergadering, waarbij ook altijd iemand van gegevensbescherming aanwezig is. Tijdens deze vergadering kan de Raad worden geïnformeerd over de stand van zaken op het gebied van informatiebeveiliging en gegevensbescherming.

Activiteiten

Inzicht in verwerkingen
In het verwerkingsregister worden op procesniveau de verwerkingsactiviteiten beschreven die onder de verantwoordelijkheid van de gemeente vallen. Het gaat hierbij om de gehele levenscyclus van de gegevens, van verkrijgen/creëren tot en met het vernietigen ervan. Het register is in beheer bij de Privacy Officer. De verantwoordelijkheid voor het vullen en actualiseren van het register, wat betreft de eigen verwerkingen, ligt bij de proceseigenaren binnen de Teams.

Risicobeoordeling
De ene verwerking is de andere niet. Een inbreuk op de persoonsgegevens zal voor de ene verwerking, bijvoorbeeld een aanvraag voor het kappen van een boom, minder ingrijpend zijn dan voor een andere verwerking, zoals een aanvraag voor een rolstoel voor een kind met een handicap. Verwerkingen waarbij te verwachten is dat een inbreuk ingrijpend zal zijn, gaan we nader onderzoeken. Een dergelijk onderzoek heet een Data Protection Impact Assessment (DPIA).

De DPIA is één van de primaire instrumenten die de gemeente tot haar beschikking heeft voor het sturen op gegevensbeschermingsrisico's en het afleggen van verantwoording over de gegevensbescherming.

Door een DPIA uit te voeren kunnen risico's al voordat de verwerking plaatsvindt aan het licht komen. Door maatregelen, die de risico's kunnen beperken dan wel wegnemen, te bedenken en door te voeren kan een verwerking een stuk veiliger plaatsvinden. Dit kunnen technische oplossingen zijn, maar het kan ook gaan om aanpassingen in de werkinstructie of in de procedure. Wanneer blijkt dat de DPIA te veel risico's aantoont, die niet ingeperkt kunnen worden, dan mag deze verwerking niet (meer) worden uitgevoerd.

• De verantwoordelijkheid voor het uitvoeren van DPIA's ligt bij de 1e-lijn. Deze wordt daarin ondersteund door de 2e-lijn (Privacy Officer met advies van de CISO)
• Afgeronde DPIA's worden ter beoordeling voorgelegd aan de FG
• Omgang met vastgestelde risico's en adviezen van de FG staat beschreven in het document Beschrijving DPIA proces
Het uitvoeren van een DPIA is geen éénmalige exercitie. Een DPIA moet periodiek herijkt worden, en bijgewerkt wanneer het onderliggende proces gewijzigd wordt.
Ook bestaande verwerkingen waar nog geen DPIA op is uitgevoerd komen aan bod.
In het implementatieplan is vastgelegd welke inspanning er wordt geleverd op het uitvoeren van DPIA's.

Passende technische en organisatorische maatregelen

Privacy- by -design en privacy by default
De gemeente treft tijdig de benodigde technische en organisatorische maatregelen om de gegevensbescherming te waarborgen. Hierdoor zorgen we er aan de voorkant voor dat er zich geen problemen met impact op de betrokkene voordoen. Dit heet Privacy by Design. Een onderdeel hiervan is Privacy by Default: het gebruik van de meest privacy-vriendelijke standaardinstellingen.
De gemeente borgt Privacy by Design door het meenemen van gegevensbeschermings-overwegingen bij inkoopprocedures, bij bespreking van wijzigingen in het Change Advisory Board (CAB) en bij het vormgeven van processen en procedures.
Om periodiek te toetsen of de geïmplementeerd maatregelen effectief zijn wordt de PDCA-cyclus gehanteerd.

Incidentenmanagement
Het beheer van het datalekregister, het doen van feitenonderzoek naar aanleiding van een melding van een vermoed datalek, het melden en administreren van datalekken en het adviseren over verbetermaatregelen naar aanleiding hiervan, behoort tot de werkzaamheden van de Privacy Officer. Wel blijft de verantwoordelijkheid voor het melden, de feitelijke afhandeling, waaronder het informeren van betrokkenen, en het implementeren van verbetermaatregelen bij de eerste lijn liggen.

Gemeente Rhenen moedigt het melden van potentiële beveiligingsrisico's of datalekken aan. Meldingen van beveiligingsrisico's worden gezien als een kans om het proces, de werkwijze en de dienstverlening

te verbeteren. Een minimaal gevuld register van datalekken kan een indicator zijn dat de bereidheid tot melden laag is.

Transparantie & rechten van betrokkenen
De Privacy Officer ondersteunt de organisatie in het laagdrempelig en begrijpelijk informeren van inwoners, medewerkers en andere betrokkenen over de verwerking van hun gegevens. Ook kan de Privacy Officer de organisatie ondersteunen wanneer een betrokkene diens rechten onder de AVG uitoefent, zoals: inzage, correctie of verwijdering van persoonsgegevens

Bewustwording
Het stimuleren van bewustwording bij medewerkers en partners van de gemeente over veilige en verantwoorde verwerking van persoonsgegevens.
Iedere medewerker krijgt binnen 3 maanden na indiensttreding een training, waarin ook uitdrukkelijk aandacht is voor de te beschermen gegevens ("kroonjuwelen").
De manager is in de eerste plaats verantwoordelijk voor het kennisniveau van de medewerkers. De activiteiten op het gebied van training en bewustwording en de monitoring en opvolging daarvan staan nader uitgewerkt in het implementatieplan Privacy. In de ideale situatie loopt regie op en monitoring van trainingen en bewustwording via Personeel en Organisatie, dit om verdere professionalisering van medewerkers goed te borgen.

Ketenregie
Om wettelijke taken uit te kunnen voeren, kan het nodig zijn om gegevens te delen met derden. Afhankelijk van haar rol in de gegevensverwerking moet de gemeente ook bij het verstrekken van gegevens aan andere organisaties de gegevensbescherming waarborgen.
Bij het aangaan van gegevensverwerking in ketens zoals samenwerkingsverbanden of het inschakelen van verwerkers treft de gemeente daarom de nodige maatregelen in de vorm van contractuele afspraken, procedures en technische maatregelen om de gegevensbescherming te borgen.

Tactisch beleid gegevensbescherming
Nadere uitwerking van gegevensbeschermingsbeleid, bijvoorbeeld een werkproces, worden opgenomen in een tactische beleidsbundel, waarop ook wat makkelijker aanpassingen in het kader van de Plan-Do-Check-Act cyclus kunnen worden gemaakt.

Definities

Voor een uitputtende lijst wordt verwezen naar de website van de Autoriteit voor Persoonsgegevens.

Autoriteit Persoonsgegevens (AP) - De Autoriteit Persoonsgegevens is de landelijke toezichthouder op het gebied van privacy.
Betrokkene - De betrokkene is degene wiens gegevens worden verwerkt.
Functionaris Gegevensbescherming (FG) - De FG is een onafhankelijk toezichthouder. De FG toetst zowel structureel en incidenteel op naleving van de AVG, gerelateerde wetgeving zoals de Wpg en interne beleidsafspraken. Daarnaast heeft de FG een ombudsmanfunctie.
Persoonsgegeven - Een persoonsgegeven bevat informatie die direct of indirect over een persoon gaan.
Verwerken - Het verwerken van een persoonsgegeven houdt iedere handeling met een persoonsgegeven in. Dit kan bijvoorbeeld zijn het verzamelen, vastleggen, raadplegen, gebruiken en verstrekken van een persoonsgegeven.
Verwerker - Een verwerker is een persoon of organisatie die persoonsgegevens verwerkt namens de gemeente Rhenen.
Verwerkingsverantwoordelijke - In de gemeente Rhenen is het college van Burgemeester en Wethouders verantwoordelijk voor het verwerken van persoonsgegevens. Dit betekent dat het college bepaalt wat er met de gegevens gebeurt. Als het gaat om openbare orde is de burgemeester verantwoordelijk.
Afkortingen
AP Autoriteit Persoonsgegevens
AVG Algemene Verordening Gegevensbescherming
DPIA Data Protection Impact Assessment
FG Functionaris voor gegevensbescherming
IMT Integraal Management Team
VNG Vereniging van Nederlandse gemeenten

Wpg Wet Politiegegevens

Voorzitter
G.A. Kaai

Gemeentesecretaris
P. Bonthuis

Vastgesteld in de collegevergadering van 23 september 2025