GEMEENTE WEST BETUWE

GEMEENTEBLAD

Officiële uitgave van de gemeente West Betuwe

Nr. 143133

5 april

2023

Privacybeleid gemeente West Betuwe

Privacy is een grondrecht. Een voorwaarde om vrij te zijn in wie je bent en wat je doet.

Privacy gaat erover dat mensen regie houden over hun gegevens. En dat bijvoorbeeld één foto waar iemand als dronken tiener op staat, niet zijn of haar toekomst bepaalt.

Het gaat erom dat we niet continu gevolgd worden, dat onze medische gegevens veilig zijn, dat we iets kunnen doen tegen een automatisch genomen besluit over ons.

Het gaat over zeggenschap over onze eigen persoonsgegevens.

Met deze uitspraken geeft de Autoriteit Persoonsgegevens (AP) goed aan waarom bescherming van persoonsgegevens in onze samenleving van belang is. Dit grondrecht, dat is vastgelegd in diverse internationale verdragen en ook in onze Grondwet, is binnen EU-verband vertaald naar de Algemene Verordening Gegevensbescherming (AVG), die vanaf 25 mei 2018 rechtstreeks als wet geldt. Het privacybeleid is een vertaling van de uitgangspunten van de AVG. Het geeft richting aan de bescherming van persoonsgegevens binnen onze organisatie.

1. Inleiding

Binnen de gemeente West Betuwe (hierna genoemd: gemeente) wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens van burgers worden voornamelijk verzameld voor het goed uitvoeren van de gemeentelijke (meestal wettelijke) taken. Wanneer het nodig is om met andere partijen samen te werken, verwerkt de gemeente soms gegevens van (keten)partners. Ook verwerkt de gemeente als werkgever persoonsgegevens van haar medewerkers. Al deze betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met hun persoonsgegevens omgaat.

Technologische ontwikkelingen, globalisering en een steeds meer digitale overheid stellen hogere eisen aan de bescherming van persoonsgegevens en privacy. Het dataverkeer neemt toe en er worden meer gegevens verzameld en gedeeld. Ook de hoeveelheid gevoelige informatie die van personen wordt vastgelegd neemt toe, evenals de risico's van bijvoorbeeld cybercrime. De samenleving wordt steeds kritischer en burgers hebben steeds meer behoefte aan rechten om inzicht te krijgen in de verwerking van hun persoonsgegevens.

Het doel van de Algemene Verordening Gegevensbescherming (AVG) is met name om een goede bescherming van persoonsgegevens te bieden en het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.

Na de paragrafen in dit hoofdstuk waarin kort wordt ingegaan op het verwerken van persoonsgegevens en het juridisch kader dat daarop van toepassing is, komen in de volgende hoofdstukken achtereenvolgens aan de orde: de algemene uitgangspunten van het privacybeleid, het privacymanagement, informatiebeveiliging, samenwerking met andere partijen, bewustwording en tot slot toezicht en rapportage.

1.1 Wat houdt het verwerken van persoonsgegevens in?

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de 'betrokkene'). Dit betekent dat deze informatie direct over iemand gaat of naar deze persoon te herleiden is.

Er is al snel sprake van het verwerken van persoonsgegevens. Onder andere verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens: het valt allemaal onder het verwerken van persoonsgegevens.

Dus alleen al het 'bekijken' van informatie is een verwerking die valt onder de AVG. Dit geldt ook voor het samenstellen van een nieuwe verwerking uit meerdere bronsystemen (het combineren van gegevens). Het is van belang om hiervoor de juiste rechtmatige grondslag te hebben.

1.2 Wie verwerken persoonsgegevens?

In de gehele gemeentelijke organisatie worden persoonsgegevens verwerkt. Dit varieert van het gebruik van een beperkte gegevensverzameling, zoals een lijst met email-adressen door communicatie, tot het gebruik van grote gegevensverzamelingen, zoals de Basisregistratie Personen (BRP) door burgerzaken.

De gegevens worden in de basis in de eigen (vak)applicaties vastgelegd, maar kunnen ook via het centrale gegevensmagazijn worden verwerkt. Via dit centrale gegevensmagazijn is het mogelijk om gegevens afkomstig uit basisregistraties (BRP, BAG) te verstrekken aan aangesloten applicaties. Daarnaast kunnen persoonsgegevens in een datawarehouse worden opgenomen. Persoonsgegevens worden dan vanuit verschillende vakapplicaties samengevoegd om op die manier managementrapportages en beleidsinformatie op te stellen.

1.3 Reikwijdte privacybeleid

De gemeente hecht veel waarde aan het zorgvuldig, rechtmatig en veilig verwerken van persoonsgegevens. Het bestuur en management zijn primair verantwoordelijk om dit te waarborgen.

Dit beleid is van toepassing op de gehele organisatie en geldt voor alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Het is in lijn met het algemene beleid van de gemeente en de relevante lokale, nationale en Europese wet- en regelgeving. In dit algemene privacybeleid staan kaders beschreven voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en de omgang ermee.

Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor privacy op tactisch niveau en werkinstructies op operationeel niveau (bijvoorbeeld privacybeleid voor het sociaal domein). Verder worden naar aanleiding van dit beleid werkprocessen opgesteld en vastgesteld die als handvat fungeren om het beleid in de dagelijkse praktijk toe te passen.

Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente gegevens verwerkt of laat verwerken en is van toepassing op alle taken en processen waarvoor de gemeente verantwoordelijk is. Hieronder valt ook de uitwisseling van persoonsgegevens door de gemeente. Daarnaast maakt de gemeente op een aantal terreinen aparte samenwerkingsafspraken met haar partners.

1.4 Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. De AVG biedt hiervoor het wettelijk kader, samen met de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Als algemene regel geldt dat persoonsgegevens op een behoorlijke en zorgvuldige manier moeten worden verwerkt. Degene die verantwoordelijk is voor de gegevensverwerking moet daarbij transparant zijn. De AVG bepaalt verder dat persoonsgegevens alleen voor een specifiek omschreven doel mogen worden verwerkt en niet voor andere doelen dan waarvoor zij verzameld zijn. Daarbij bepaalt de AVG dat deze gegevens alleen mogen worden verwerkt als dat noodzakelijk is om het specifiek beschreven doel te bereiken en dat zo min mogelijk gegevens worden verwerkt. Dat houdt ook in dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verzameld[1].

De AVG is een algemene wet, met algemene bepalingen en uitgangspunten. In specifieke wetten (bijvoorbeeld de Jeugdwet, Wmo en Participatiewet) zijn ook bepalingen over het verwerken van persoonsgegevens opgenomen.

De bepalingen in specifieke (sectorale) wetgeving over de verwerking van persoonsgegevens geven een specifieke invulling van de bepalingen van de AVG. Zo mogen op grond van de AVG medische gegevens alleen worden verwerkt als hiervoor een wettelijke grondslag aanwezig is; deze grondslag is dan opgenomen in de specifieke wet. Maar dat neemt niet weg dat de algemene uitgangspunten van de AVG, zoals ‘niet meer gegevens verwerken dan nodig’, ‘alleen indien nodig’ en ‘niet langer dan nodig’, nog steeds gelden en moeten worden vertaald naar werkprocessen.

1.5 Raakvlakken en overlap met andere beleidsthema’s

Het privacybeleid van de gemeente heeft raakvlakken met andere beleidsthema’s of vertoont hiermee overlap.

1) *Deze algemene uitgangspunten zijn terug te vinden in de artikelen 5 en 6 van de AVG en de uitgangspunten inzake transparantie in de artikelen 13 en 14 van de AVG. Beide onderdelen worden in paragraaf 2.2 nader uitgewerkt.*

Integriteitsbeleid
Privacybeleidsvoering is gekoppeld aan de beginselen van behoorlijk bestuur en heeft daardoor raakvlakken met het gemeentelijke integriteitsbeleid (Richtlijnen voor integer handelen door ambtenaren - Gedragscode West Betuwe).

Kwaliteitsbeleid
Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratie is randvoorwaardelijk voor een klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteits- en risicomanagement
Continuïteits- en risicomanagement is gericht op het tegengaan van afbreuk- en aansprakelijkheidsrisico's en het voorkomen dat processen stagneren.
Dit zou bij de desbetreffende gegevensverwerkingen kunnen leiden tot inbreuken op de bescherming van persoonsgegevens.

Informatiebeveiliging
Het beschermen van persoonsgegevens kan niet geborgd worden zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom samen met het informatiebeveiligingsbeleid.

2. Privacybeleid

2.1 Visie op privacy
Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid. Het is een grondrecht en vormt een vereiste voor het kunnen uitoefenen van andere vrijheden, zoals de vrijheid van meningsuiting en persvrijheid. De gemeente West Betuwe wil het belang van privacy uitdragen en een betrouwbare overheid zijn. Hieraan geeft ze invulling door in haar handelen de persoonlijke levenssfeer van betrokkenen te eerbiedigen, transparant te zijn over de manier waarop ze persoonsgegevens verwerkt en door te zorgen dat burgers hun privacyrechten kunnen uitoefenen.

2.2 Uitgangspunten verwerken persoonsgegevens
De gemeente houdt zich bij het verwerken van persoonsgegevens conform de AVG aan de volgende uitgangspunten[2]:

Rechtmatige grondslag
De gemeente mag alleen persoonsgegevens verwerken indien hiervoor een rechtmatige grondslag bestaat. Deze rechtmatige grondslag is in de regel gelegen in de uitoefening van haar taken van algemeen belang/uitoefening van openbaar gezag.
In sommige gevallen verwerkt ze gegevens om een overeenkomst uit te voeren of op basis van toestemming.

Ten aanzien van het gebruik van de website verwerkt de gemeente persoonsgegevens voor de uitvoering van wettelijke verplichtingen (informatievoorziening aan het publiek) of op basis van een gerechtvaardigd belang (van administratieve aard[3]). In sommige gevallen kan dit ook plaatsvinden op basis van toestemming.

De gemeente verwerkt vanuit haar wettelijke taken ook bijzondere persoonsgegevens. Bijvoorbeeld gegevens over iemands gezondheid voor de aanvraag van een hulpmiddel in het kader van de Wmo. Dit is alleen toegestaan als hiervoor in een specifieke wet een grondslag is gegeven. Is deze grondslag er niet, dan vindt een dergelijke verwerking niet plaats.

Op grond van de Wet algemene bepalingen burgerservicenummer (Wabb) is de gemeente bevoegd om het burgerservicenummer (BSN) te verwerken wanneer dit noodzakelijk is voor het uitvoeren van een overheidstaak[4].

Doelbinding

2) *Zie de artikelen 5 en 6 van de AVG.*
3) *Let op: het gebruik van 'gerechtvaardigd belang' als grondslag is zeer beperkt en mag niet leiden tot vergaande verwerking van persoonsgegevens binnen de organisatie.*
4) *Dit is in overeenstemming met het bepaalde in artikel 87 AVG en artikel 46 van de Uitvoeringswet AVG.*

Met doelbinding wordt bedoeld dat gegevens alleen worden verwerkt voor het doel waarvoor ze zijn verzameld. Als gegevens toch voor andere doelen worden gebruikt, wordt beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel van verzamelen van de gegevens[5].

Persoonsgegevens worden veelal verwerkt in vakapplicaties. Soms zijn applicaties verbonden met andere applicaties. Zo is de applicatie van het sociaal domein verbonden met de applicatie van de afdeling financiën in verband met het doen van betalingen. Hierbij worden persoonsgegevens uitgewisseld. Ook hiervoor gelden de regels van de AVG (bijvoorbeeld 'alleen indien nodig' en 'niet meer dan nodig'). Om dit goed in beeld te krijgen en te houden beschikt de gemeente over een geactualiseerd overzicht van het applicatielandschap.

Transparantie

De gemeente is transparant over hoe ze persoonsgegevens verwerkt[6]. Hierdoor weten burgers en personen van wie de gemeente persoonsgegevens verwerkt, door wie de gegevens worden verwerkt, waarom dit gebeurt en welke maatregelen genomen worden om zorgvuldig met de gegevens om te gaan.

De belangrijkste manieren om betrokkenen te informeren over de verwerking van persoonsgegevens zijn:
- het geven van algemene informatie bij inschrijving en op de website;
- het geven van aanvullende informatie (door middel van bijvoorbeeld foldermateriaal) bij het aanvragen van specifieke diensten;
- het hebben van een privacyverklaring, inclusief cookieverklaring op de gemeentelijke websites;
- het bieden van laagdrempelige mogelijkheden om inzage te krijgen in de verwerking van persoonsgegevens.

Betrokkenen worden in ieder geval geïnformeerd over:
- wie verantwoordelijk is voor de gegevensverwerking met contactgegevens;
- de contactgegevens van de Functionaris Gegevensbescherming;
- de doeleinden en rechtsgrond(en) van de gegevensverwerking;
- (indien van toepassing:) de ontvangers;
- (indien van toepassing:) nadere informatie met betrekking tot eventuele doorgifte van persoonsgegevens naar een derde land of internationale organisatie;
- hoelang gegevens bewaard worden;
- hoe wordt omgegaan met de rechten van betrokkenen.

Dataminimalisatie en proportionaliteit (niet meer dan nodig, alleen indien nodig, niet langer dan nodig)
De gemeente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel en streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Als de gemeente de gegevens niet meer nodig heeft, vernietigt zij deze, tenzij er een wettelijke verplichting is om de gegevens langer te bewaren (niet langer dan nodig).

Soms worden bewaartermijnen genoemd in specifieke wetten waarvoor gegevensverwerking nodig is; in andere gevallen bepaalt de Archiefwet de bewaartermijnen. De gemeente vernietigt in die gevallen de gegevens zodra de wettelijke bewaartermijn en/of de termijn uit de selectielijst van de VNG is afgelopen.

Vóór het verwerken van de gegevens bepaalt de gemeente of het doel van de verwerking niet op een andere, minder ingrijpende manier bereikt kan worden dan door het verwerken van de persoonsgegevens (subsidiariteit). Soms kunnen doelen ook worden bereikt door bijvoorbeeld geanonimiseerde informatie over een casus uit te wisselen. In dat geval worden er geen persoonsgegevens uitgewisseld.

Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens. Gegevens worden vertrouwelijk behandeld en op de juiste manier beveiligd. Dit gebeurt conform de bepalingen van de Baseline Informatiebeveiliging Overheid (BIO) die voor gemeenten verplicht zijn.

De gemeente treft maatregelen om de kwaliteit van de gegevens te borgen; onder 'kwaliteit' wordt verstaan dat ze juist, nauwkeurig en actueel zijn. Voordat gegevens worden verwerkt vinden er (geau-

5) *Zie artikel 6 lid 4 AVG.*
6) *Verplichting op grond van de artikelen 13 en 14 van de AVG.*

tomatiseerde) controles plaats om te voorkomen dat personen niet goed benaderd worden (denk aan het versturen van brieven naar een oud adres, het versturen van brieven met een verkeerde tenaamstelling of het versturen van een brief naar een overledene).

In ieder geval zijn de volgende maatregelen getroffen:
- Bij de invoer van gegevens vindt er een kwaliteitscontrole plaats door gegevens te verifiëren.
- ICT-systemen valideren gegevens door middel van invoercontroles.
- ICT-systemen zijn daar waar persoonsgegevens worden gebruikt veelal direct of indirect
- gekoppeld aan de BRP, zodat men automatisch beschikt over actuele gegevens. Als deze koppeling niet mogelijk is, worden de gegevens in de BRP handmatig geverifieerd voordat zij worden gebruikt.
- Betrokkenen hebben de mogelijkheid om gegevens in te zien en te laten corrigeren indien nodig.

Delen met derden
In het geval van samenwerking met externe partijen waarbij sprake is van verwerking van persoonsgegevens maakt de gemeente afspraken over de eisen waaraan gegevensuitwisseling moet voldoen. Deze afspraken voldoen aan de wet. De gemeente controleert jaarlijks steekproefsgewijs het nakomen van de gemaakte afspraken.

Integrale dienstverlening
In beginsel verwerkt de gemeente persoonsgegevens alleen voor het doel waarvoor ze zijn verzameld en worden gegevens niet gedeeld met medewerkers die daarbij niet betrokken zijn. Om burgers met complexe vraagstukken goed te kunnen ondersteunen is soms echter een samenhangende aanpak noodzakelijk. Voor deze integrale aanpak kan het nodig zijn om persoonsgegevens te delen met medewerkers die een andere wet/taak uitvoeren. Wanneer dit gebeurt wordt de betrokkene hiervan vooraf op de hoogte gebracht. Zo kan het voor de uitvoering van de Jeugdwet van belang zijn om te weten dat er ook een schuldhulpverleningstraject loopt. Is dat het geval, dan worden alleen die gegevens die voor de jeugdhulp relevant zijn in het jeugddossier vastgelegd.

Rechten van betrokkenen
De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken, maar ook de rechten van personen van wie de gegevens worden verwerkt. Hieronder een korte opsomming van deze rechten[7]:
- Recht op inzage
- Recht op rectificatie
- Recht op gegevenswissing (vergetelheid)
- Recht op beperking van de verwerking
- Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking
- Recht op overdraagbaarheid van gegevens
- Recht op bezwaar
- Recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit

De gemeente verstrekt onverwijld maar in ieder geval binnen een maand na ontvangst van een verzoek informatie over of, en zo ja op welke wijze, gevolg aan dat verzoek wordt gegeven. In complexe situaties kan deze termijn worden verlengd met twee maanden[8].

Het voert te ver om al deze rechten hier inhoudelijk te behandelen. Op basis van nieuwe richtlijnen en jurisprudentie zal de inhoud continu aan verandering onderhevig zijn. Voor de diverse rechten gelden voorwaarden en deze kennen wettelijke beperkingen (zo is bijvoorbeeld het recht op gegevenswissing niet van toepassing op registraties in de BRP).
De gemeente richt werkprocessen in om zorg te dragen voor een juiste en tijdige afhandeling van verzoeken van betrokkenen. Via de website worden betrokkenen geïnformeerd over deze rechten en wordt hun de mogelijkheid geboden om op eenvoudige wijze gebruik te maken van deze rechten.

Klachten van burgers
Voor burgers is het mogelijk om klachten over de toepassing van de AVG in te dienen bij de gemeente en bij de Autoriteit Persoonsgegevens. Binnen de gemeente worden deze klachten conform de reguliere klachtenprocedure afgehandeld. Daarbij wordt de functionaris gegevensbescherming om advies gevraagd.

Register van Verwerkingen

7) *Zie de artikelen 15 t/m 22 van de AVG.*
8) *Artikel 12 lid 3 AVG.*

De gemeente heeft een register van verwerkingen overeenkomstig artikel 30 AVG opgesteld en houdt dit actueel.

Privacy by design en privacy by default
Voordat met een nieuwe gegevensverwerking wordt gestart, zorgt de gemeente ervoor dat zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens wordt afgedwongen. Dit heet 'privacy by design'. Hierbij wordt onder andere gekeken naar de noodzaak van deze gegevens voor het te behalen doel en de benodigde beveiliging van de persoonsgegevens.

Een onderdeel van 'privacy by design' is 'privacy by default'. Hiermee wordt bedoeld dat de standaard-instellingen van een systeem (denk bijvoorbeeld aan de mogelijkheid om twee-factor-authenticatie in te schakelen) zo privacyvriendelijk mogelijk moeten zijn.

Gegevensbeschermingseffectbeoordeling /Data Protection Impact Assessment (DPIA)
Op grond van de AVG is de gemeente verplicht om in een aantal gevallen vóór de verwerking van de gegevens een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren. Het uitvoeren van een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de personen van wie de gemeente gegevens verwerkt[9].
Bij de beoordeling hiervan maakt de gemeente gebruik van de beoordelingscriteria die hiervoor zijn opgesteld door het Europees Comité voor gegevensbescherming (European Data Protection Board - EDPB) en door de Autoriteit Persoonsgegevens (AP). De AP heeft een lijst opgesteld van verwerkingen waarvoor een DPIA verplicht is. Deze lijst is terug te vinden op de website van de AP.

Een DPIA moet voorafgaand aan de verwerking worden uitgevoerd. Daarnaast heeft de AP aangegeven dat een DPIA eens per drie jaar herhaald moet worden of eerder/vaker, als er wijzigingen zijn die dit noodzakelijk maken.

De gemeente zorgt ervoor tijdig in beeld te brengen voor welke verwerkingen een DPIA verplicht is. Met gebruikmaking van het register van verwerkingen bepaalt de procesverantwoordelijke of een DPIA verplicht is en wanneer deze moet worden uitgevoerd. Het is van belang om hierbij ook aan te sluiten bij ontwikkelingen rond een verwerking, zoals:
- nieuwe wettelijke bepalingen, taken of grote wijzigingen;
- organisatiewijzigingen of samenwerkingen met derden, dan wel overdracht van taken;
- de aanschaf van nieuwe software of ICT-apparatuur.

Samenwerkingsverbanden
De gemeente werkt samen in regionaal verband, bijvoorbeeld in samenwerkingen op het gebied van zorg en van veiligheid, zoals het Veiligheidshuis. De gemeente zorgt ervoor dat zij met deze samenwerkingspartners afdoende afspraken maakt om de privacy te waarborgen.
Vóór de deelname in een (nieuw) samenwerkingsverband voert zij een DPIA uit om de risico's van deelname aan het samenwerkingsverband te analyseren en hierop maatregelen te nemen.

3. Privacy management

Voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet is goed privacy management noodzakelijk. Het gaat hierbij om vragen als:
- Hoe is privacy ingebed in de organisatiestructuur?
- Bij wie ligt het proceseigenaarschap?
- Wie houdt toezicht op de naleving?

Het uiteindelijke doel is dat privacy een vanzelfsprekend onderdeel van de bedrijfsvoering wordt. Daarbij is het uitgangspunt een inrichting die zo privacybestendig mogelijk is.

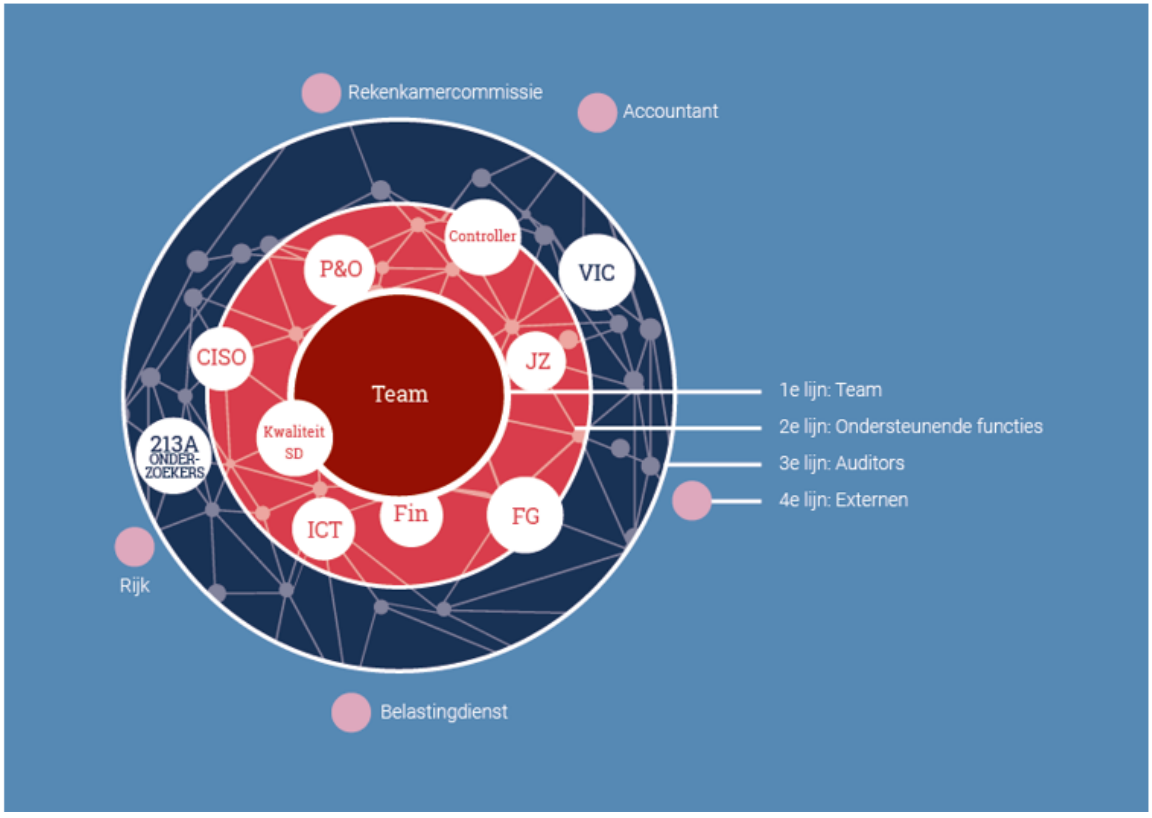
3.1 Taken en verantwoordelijkheden (de privacy governance)
Het college is eindverantwoordelijk voor de naleving van privacywetgeving. Binnen het college ligt deze verantwoordelijkheid bij de portefeuillehouder bedrijfsvoering. Het college stelt het privacybeleid vast.

De organisatie heeft de verantwoordelijkheid om het privacybeleid uit te voeren. Hiervoor wordt een afweging van belangen en risico's bij de verwerking van persoonsgegevens gemaakt, zodat dit behoorlijk, zorgvuldig en in overeenstemming met de wet plaatsvindt.

9) *Artikel 35 AVG.*

Het college legt over de uitvoering van het privacybeleid verantwoording af aan de gemeenteraad en zorgt voor een zodanige documentatie van beleid en maatregelen dat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.

De directie is ambtelijk eindverantwoordelijk voor de uitvoering van het privacybeleid.
In onze visie op control hebben we eerder aangegeven dat we de ambtelijke taken en verantwoordelijkheden inrichten volgens drie verantwoordelijkheidslijnen:



Uit de controlvisie:

1. Het management is primair verantwoordelijk voor de realisatie van de strategie en voor de daarvan afgeleide doelstellingen. Het lijnmanagement op de diverse organisatieniveaus is dus ook primair verantwoordelijk voor de goede sturing en beheersing van de organisatie, voor het managen van de risico's die met de bedrijfsvoering samenhangen en voor de volledigheid en betrouwbaarheid van de verantwoordingsinformatie.
2. De tweede lijn ondersteunt het management bij het koers houden en de inrichting van de organisatie en processen, het gaat om ondersteunende functies op het gebied van de bedrijfsvoering en kwaliteitszorg.
3. De derde lijn in het model staat voor de interne auditfunctie: deze geeft de managers aanvullende zekerheid over de kwaliteit van sturing en beheersing.

Eerste lijn: teamleiders
De teamleider is ervoor verantwoordelijk dat de gemeentelijke taakuitoefening binnen de grenzen van dit privacybeleid plaatsvindt en rapporteert hierover aan de directie, die op haar beurt rapporteert aan het college.

De teamleider is proceseigenaar. Proceseigenaren voeren regie over hun proces(sen).
De proceseigenaar kan verantwoordelijkheden beleggen bij medewerkers. De teamleider kan binnen zijn teams de rol van privacy contactpersoon inrichten. Deze rol wordt in ieder geval geborgd voor de teams Publiek en Sociaal.

Tweede lijn: de Privacy officer
De Privacy officer zorgt voor een actueel privacybeleid en de implementatie daarvan. Daarna adviseert deze gevraagd en ongevraagd over mogelijke privacy issues binnen de gemeente West Betuwe. Ook is de Privacy officer verantwoordelijk voor het opstellen en uitvoeren van het bewustwordingsprogramma, de inrichting van het verwerkingsregister en het uitvoeren van data privacy impact assessments (DPIA's).

De Privacy Officer houdt geen toezicht op de naleving van het privacybeleid, maar kan hier wel over adviseren. De Privacy officer rapporteert over privacy incidenten en datalekken aan de FG.

Derde lijn: de Functionaris gegevensbescherming (FG) en concerncontroller
De functionaris gegevensbescherming controleert of er conform de AVG wordt gewerkt.
De concerncontroller heeft een eigen verantwoordelijkheid om zich te laten informeren over zaken die voor een goede rolinvulling van belang zijn. Daarom schuift de concerncontroller in de basis aan bij de belangrijkste overleg- en besluitvormingsorganen. Ook organiseert de controller een overleg met functies uit de tweede lijn, het controlteam, waaronder in het kader van het privacybeleid de privacy officer. In dit overleg wordt de voortgang van de verbeterplannen jaarlijks gemonitord.

4. Informatiebeveiliging

Om zorgvuldig met persoonsgegevens te kunnen omgaan moeten er passende, beschermende maatregelen worden getroffen[10]. Deze maatregelen moeten de geheimhouding en beveiliging van de gegevens borgen. Ze gelden voor iedereen die onder verantwoordelijkheid van het college van de gemeente werkt: interne medewerkers, verwerkers en subverwerkers. De maatregelen gelden ook voor diensten en goederen die onderdeel zijn van de beveiliging, zoals de beveiliging van het pand, de schoonmaak of de leveranciers van hardware.

Op grond van de meldplicht datalekken[11] meldt het college een beveiligingsincident bij de AP, tenzij het niet aannemelijk is dat de inbreuk op de beveiliging een privacyrisico inhoudt. De gemeente houdt een datalekregister bij[12]. De procedure rond de meldplicht van datalekken is uitgewerkt in een handleiding voor de medewerkers van de gemeente.

4.1 Geheimhouding
Alle personen, die onder het gezag van het college werken, zijn tot geheimhouding verplicht. Elke werknemer in vaste dienst legt bij indiensttreding een eed of belofte af als onderdeel van de arbeidsovereenkomst. Daarnaast wordt bij de ondertekening van de arbeidsovereenkomst een geheimhoudingsverklaring getekend. Inhuurkrachten tekenen in ieder geval bij de ondertekening van de inhuurovereenkomst een geheimhoudingsverklaring.

Het college heeft ook een gedragscode integriteit voor medewerkers vastgesteld. Hierin zijn (onder meer) richtlijnen opgenomen voor het vertrouwelijk omgaan met privacygevoelige informatie.

Wanneer het voor hun functie nodig is dat medewerkers toegang krijgen tot de Basisregistratie Personen of tot Suwinet, dan tekenen zij een specifieke verklaring omtrent geheimhouding en het juiste gebruik van deze systemen.

Verwerkers en externe partijen worden door middel van verwerkersovereenkomsten en contracten verplicht tot geheimhouding. In alle contracten met leveranciers, verwerkers en overige externen die toegang krijgen tot het pand of tot de systemen is een bepaling met betrekking tot geheimhouding opgenomen.

4.2 Informatiebeveiliging
Voor informatiebeveiliging geldt de norm van de Baseline Informatiebeveiliging
Overheid (BIO). De gemeente volgt hiermee de richtlijnen die door de Ministerraad in december 2018 zijn vastgesteld voor overheidsorganisaties, waaronder gemeenten.

Er is hiervoor een strategisch en tactisch informatiebeveiligingsbeleid opgesteld, dat iedere drie jaar wordt herzien en opnieuw wordt vastgesteld.

5. Samenwerken met andere partijen

De gemeente werkt in meerdere situaties samen met andere partijen. Afhankelijk van de samenwerkingsrelatie wordt dit vastgelegd in convenanten, in verwerkersovereenkomsten of in een overeenkomst gezamenlijke verwerkingsverantwoordelijkheid.

10) *Zie artikel 24 AVG.*
11) *Zie artikel 33 AVG.*
12) *Zie artikel 33 lid 5 AVG.*

5.1 Convenanten

Daar waar partijen samenwerken maar zelf verantwoordelijk zijn en blijven voor hun eigen verwerkingen is een convenant van belang om afspraken te maken over bijvoorbeeld de wijze waarop persoonsgegevens worden uitgewisseld.

In een dergelijk convenant gaat het om de onderlinge verantwoordelijkheden en ook om hoe er moet worden omgegaan met onder andere de rechten van betrokkenen en met datalekken. Het zijn vooral werkafspraken over de samenwerking en uitwisseling van persoonsgegevens. Een convenant biedt geen rechtsgeldige grondslag voor een uitwisseling van persoonsgegevens. De grondslag hiervoor vloeit voort uit de rechtmatige verwerking door de partijen en moet door partijen zelf worden ingevuld.

5.2 Verwerkersovereenkomsten

Verwerkers zijn derden die in opdracht van de gemeente persoonsgegevens verwerken zonder dat zij verwerkingsverantwoordelijke worden; denk aan het bedrijf dat gegevens van personeelsleden verwerkt om de salarissen te kunnen uitbetalen. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd. Met alle verwerkers wordt een verwerkersovereenkomst gesloten conform het VNG- standaardmodel.

5.3 Gezamenlijke verwerkingsverantwoordelijken

Het kan voorkomen dat de gemeente samen met een andere organisatie persoonsgegevens verwerkt. In dat geval wordt er een overeenkomst opgesteld waarin op transparante wijze de verantwoordelijkheden voor de nakoming van de verplichtingen uit de AVG worden vastgesteld, met name ten aanzien van de uitoefening van de rechten van betrokkenen en de informatieplicht[13].

6. Bewustwording, communicatie en evaluatie

Privacybeleid moet niet beperkt blijven tot het formuleren van uitgangspunten en door het college na te streven doelen. Alle medewerkers van de gemeente dragen in de praktijk zorg voor de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Privacy is daarmee voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. College, management en medewerkers moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van het belang van het waarborgen van de rechten van burgers.

Naast het opstellen van privacybeleid en het inrichten van werkprocessen is het belangrijk dat personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig moeten omgaan met persoonsgegevens. Daarom is het belangrijk dat de medewerkers van de gemeente zich bewust zijn van de regels en gedragsnormen rondom privacy. De gemeente ondersteunt dit proces door het ontwikkelen van bijvoorbeeld privacyprotocollen en afwegingskaders.

Om ervoor te zorgen dat medewerkers zich bewust zijn van het belang van privacy en weten hoe zij persoonsgegevens op een zorgvuldige manier moeten verwerken wordt er jaarlijks een bewustwordingsprogramma opgesteld. Hierin staan verschillende aandachtspunten met het oog op bewustwording (en het bewust blijven) bij de personen die met deze gegevens werken. Omdat het veilig omgaan met persoonsgegevens direct verband houdt met informatiebeveiliging, wordt het oppakken van bewustwording op het gebied van privacy gecombineerd met bewustwording op het gebied van informatiebeveiliging. In het bewustwordingsprogramma wordt ook aandacht besteed aan bijvoorbeeld trainingen en opschoondagen.

De gemeente streeft naar een cultuur waarin medewerkers elkaar in alle openheid aanspreken op het gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimaal privacybeleid.

Aan het eind van elk jaar wordt geëvalueerd wat de opbrengst was van het bewustwordingsprogramma, zodat hier rekening mee gehouden kan worden bij het opstellen van een dergelijk programma voor het volgende jaar.

7. Toezicht en rapportage

Jaarlijks evalueert het management de uitvoering van het privacybeleid en rapporteert hierover aan het college. Hierbij wordt aangegeven in hoeverre de gemeente (conform artikel 5 lid 2 van de AVG) voldoet aan de uitgangspunten van de AVG[14].

13) *Zie artikel 26 AVG.*
14) *Zie artikel 5 lid 2 AVG.*

De functionaris gegevensbescherming stelt voor de verantwoording van zijn werkzaamheden en bevindingen een jaarverslag op en biedt dit aan het college aan. Hij voegt hierbij een eigen visie op de door het management uitgevoerde evaluatie. Het college biedt dit verslag, met zijn reactie, ter informatie aan de gemeenteraad aan.

8. Tot slot

Dit privacybeleid treedt in werking na vaststelling door het college. Het beleid wordt iedere drie jaar geëvalueerd en indien nodig herzien.

Vastgesteld in de vergadering van burgemeester en wethouders van de gemeente West Betuwe van 1 november 2022.

De secretaris,
De burgemeester,