

Beleid verstrekking van gegevens uit de BRP

Spelregels voor de geautomatiseerde verstrekking van persoonsgegevens uit de Basisregistratie personen (BRP) aan binnengemeentelijke organen.

Inhoudsopgave

1. Inleiding
2. Verstrekkingen aan binnengemeentelijke organen
3. Stappenplan geautomatiseerde verstrekking (chronologisch)
4. Uitwerking stappenplan
 - 4.1 Behoeftes aan gegevens afkomstig uit de BRP
 - 4.2 Verstrekken en verwerken
 - 4.3 Beoordeling van de rechtmatigheid van een geautomatiseerde verstrekking
 - 4.3.1 Overheidsorganen
 - 4.3.2 Welke gegevens worden verstrekt?
 - 4.3.3 Het verder verwerken van gegevens afkomstig uit de BRP
 - 4.4 Adviesverzoek aan de privacy officer
 - 4.5 Functionaris Gegevensbescherming en rol privacy officer
 - 4.6 Informatiebeveiliging en verwerkersovereenkomst
 - 4.7 Belangenafweging en conflictbeheersing
 - 4.8 Besluit tot verstrekking en aansluiting op de BRP
 - 4.9 Controle op de rechtmatige verwerking van persoonsgegevens afkomstig uit de BRP

1. Inleiding

Deze notitie heeft betrekking op de geautomatiseerde verstrekking van persoonsgegevens uit de BRP aan binnengemeentelijke organen. Daarmee is het een uitwerking van de 'Verordening gegevensverstrekking basisregistratie personen Tiel 2014' en van het 'Reglement gegevensverstrekking Basisregistratie Personen Tiel 2020'.

Sinds 1 januari 2010 geldt voor de hele overheid, en dus ook binnen gemeenten, de verplichting om bij de uitvoering van publieke taken gebruik te maken van persoonsgegevens uit de BRP. Gelet op artikel 3.8 Wet BRP en artikel 6 lid 1 sub e van de Algemene Verordening Gegevensbescherming (AVG), kunnen gegevens uit de BRP van de gemeente Tiel aan organen van de gemeente Tiel/Bedrijfsvoeringsorganisatie West-Betuwe worden verstrekt, voor zover deze organen deze gegevens nodig hebben voor de uitvoering van hun taken.

In de praktijk vindt distributie van persoonsgegevens plaats vanuit een specifiek daarvoor ingericht gegevensmagazijn. Deze oplossing kan worden gezien als een praktische tussenstap op weg naar een oplossing waarbij gegevens altijd rechtstreeks bij de bron worden opgevraagd (common ground). Via een automatische koppeling worden via de Enterprise Service Bus (ESB) gegevens vanuit de BRP verstrekt aan het gegevensmagazijn. Vanuit het gegevensmagazijn worden via de ESB gegevens verstrekt aan de aangesloten applicaties, die nodig zijn voor de uitvoering van publieke taken.

Uitgangspunt is dat doorlevering van persoonsgegevens vanuit een gegevensmagazijn dat (mede) is gevuld met BRP-gegevens, alleen is toegestaan nadat hiervoor een formeel besluit is genomen. Het besluit, de bijbehorende belangenafweging en advisering worden vastgelegd in een dossier in het zaakstelsel.

Dit beleid beschrijft de afhandeling van verzoeken om geautomatiseerde verstrekkingen uit de BRP. Voordat tot verstrekking wordt besloten worden een aantal vaste stappen doorlopen en vindt er een belangenafweging plaats. Voor de belangenafweging is in Tiel een adviesrol weggelegd voor de privacy officer.

2. Verstrekkingen aan binnengemeentelijke organen

De rol van burgemeester en wethouders (B en W) bij lokale verstrekkingen is de volgende:

1. Het beoordelen van aanvragen van gemeentelijke organen die voor hun taak BRP-gegevens via het gegevensmagazijn willen ontvangen.
2. Het overgaan tot verstrekking van gegevens over ingezetenen.
3. In het geval van verstrekking, het vastleggen van het feit van verstrekking gedurende een periode van 20 jaar.
4. Voldoen aan verzoeken om inzage van burgers.

In Tiel is de rol van gemeentelijke verstrekker (kortweg: verstrekker) door B en W binnengemeentelijk gemandateerd aan de teammanager Publiekszaken, met een ondermandaat aan de medewerkers van het team Publiekszaken. De binnengemeentelijke geautomatiseerde verstrekking doorloopt een vast aantal stappen en een belangenafweging. Deze stappen worden in de volgende hoofdstukken verder uitgewerkt.

3. Stappenplan geautomatiseerde verstrekking (chronologisch)

1. Vanuit de dienstverlenende taakstelling van een overheidsorgaan van de gemeente (verder: afnemer) ontstaat behoefte aan persoonsgegevens afkomstig uit de BRP. De afnemer formuleert een verzoek om gegevens uit de BRP waarin de gronden en noodzaak van de verstrekking zijn beschreven en stuurt deze naar de verstrekker. In de praktijk neemt de privacybeheerder BRP het verzoek in behandeling. Het verzoek van de afnemer wordt vastgelegd in een dossier in het zaaksysteem.
2. De verstrekker adviseert de potentiële afnemer over het rechtmatig gebruik van persoonsgegevens afkomstig uit de BRP. De informatie kan gaan over rechtstreekse verstrekking uit de BRP met een raadpleegbevoegdheid of over doorlevering uit een gegevensmagazijn, met daarin gegevens die oorspronkelijk afkomstig zijn uit de BRP. Per concreet geval zal door de afnemer aangetoond moeten worden dat doorlevering vanuit het gegevensmagazijn een aantoonbare meerwaarde heeft.
3. De verstrekker verifieert of een afnemer bevoegd is de gevraagde gegevens te ontvangen. De verstrekker beoordeelt de rechtmatigheid van de verstrekking. Daarbij moet worden voldaan aan de eisen van proportionaliteit, subsidiariteit en transparantie. De afnemer verstrekt alle informatie die noodzakelijk is om tegenover betrokkenen een behoorlijke en transparante verwerking te waarborgen.
4. Ten aanzien van de verstrekking uit de BRP vraagt de verstrekker advies aan de privacy officer. Het advies van de privacy officer wordt vastgelegd in het dossier in het zaaksysteem.
5. In geval van complexe gegevensverwerking vraagt de privacy officer de Functionaris Gegevensbescherming (FG) om advies over de gewenste verstrekking. Het advies van de FG wordt vastgelegd in het dossier in het zaaksysteem.
6. Voor de informatiebeveiliging van de geautomatiseerde levering van persoonsgegevens wordt zoveel mogelijk gebruik gemaakt van gemeentelijke standaarden. De afnemer vraagt de Chief Information Security Officer (CISO) om advies over de gewenste verstrekking. Het advies van de CISO wordt vastgelegd in het dossier in het zaaksysteem. Daarbij wordt rekening gehouden met voorwaarden, zoals de normen van de Autoriteit Persoonsgegevens, de AVG en de Baseline Informatiebeveiliging Overheid (BIO). De afnemende partij voert een risicoanalyse en/of een data protection impact assessment (DPIA) uit. Bij een DPIA wordt het advies van de FG vastgelegd.
7. De verstrekker weegt de belangen af naar aanleiding van de adviezen van de privacy officer, CISO en de FG. Indien de FG, CISO en de privacy officer conflicterende adviezen of verschillen van inzicht hebben, wordt het conceptbesluit over de gegevensverwerking voorgelegd aan het college.
8. De verstrekker neemt namens B en W het formele besluit tot verstrekking van gegevens aan de afnemer. Verstrekker en afnemer gaan daarop over tot technische realisatie van de aansluiting op het gegevensmagazijn. Hiervoor wordt het proces van changemanagement opgestart via het Facility Management Informatie Systeem.
9. De verstrekker controleert periodiek de rechtmatige verwerking van persoonsgegevens afkomstig uit de BRP. De FG heeft een toezichhoudende rol ten aanzien van de verwerking van persoonsgegevens op grond van de AVG.

4. Uitwerking stappenplan

4.1 Behoeft aan gegevens afkomstig uit de BRP

De verstrekker doet slechts een marginale toets op het criterium "noodzakelijk"

Volgens de Wet BRP hebben overheidsorganen recht op BRP-gegevens als deze noodzakelijk zijn voor de uitvoering van hun publiekrechtelijke taken.

4.2 Verstrekken en verwerken

Een afnemer die behoefte heeft aan gegevens afkomstig uit de BRP moet zich realiseren dat het verwerken van persoonsgegevens gebonden is aan regels.

Een verstrekking uit de BRP vindt plaats onder het regime van de Wet BRP. Op verwerken van persoonsgegevens is de AVG altijd van toepassing. De wet BRP is een bijzondere wet en in feite een nadere uitwerking van de AVG voor persoonsgegevens uit de BRP.

Op het moment dat persoonsgegevens uit de BRP zijn verstrekt aan de afnemer is de BRP regelgeving niet meer direct van toepassing. Wel werkt deze nog door in de doelbinding. Bij voortgezet gebruik moet men immers rekening houden met het doel waarvoor men gegevens heeft verkregen. In dat kader is het verstandig bij iedere verwerking van persoonsgegevens, die direct of indirect afkomstig zijn uit de BRP, informatie in te winnen bij de verstrekker.

De afnemer is zelf verantwoordelijk voor het in een vroeg stadium inwinnen van informatie.

De inventarisatie van de voorgenomen gegevensverwerking verloopt in samenspraak met de verstrekker, waarbij ook een actieve rol van de afnemer wordt verwacht.

De verstrekker faciliteert in de vorm van het geven van informatie en het verschaffen van documentatie, met als doel dat de afnemer binnen de wettelijke grenzen op een effectieve manier gebruik kan maken van de BRP.

Voor de doorlevering vanuit het gegevensmagazijn maakt de afnemer een ICT-melding aan via het Facility Management Informatie Systeem. Hierdoor is de afdeling ICT in een vroeg stadium geïnformeerd over deze aanvraag.

De verwerking wordt op een groot detailniveau vastgelegd in een document:

- wie heeft toegang tot welke gegevens
- zoekingen
- gegevenssets
- functioneel beperkende maatregelen binnen applicaties
- etc.

Aanvullend wordt de verwerking van persoonsgegevens opgenomen in het register van verwerkingen. De afnemer meldt de verwerking aan bij de privacybeheerder van het betrokken domein.

4.3 Beoordeling van de rechtmatigheid van een geautomatiseerde verstrekking

De verstrekker stelt vast of het verzoek afkomstig is van een orgaan van de gemeente en of de gegevens nodig zijn voor de goede vervulling van hun taak (art. 3.8 Wet BRP).

4.3.1 Overheidsorganen

Het primaire doel van de BRP is het verstrekken van gegevens aan overheidsorganen. De verstrekker levert alleen gegevens aan overheidsorganen van de gemeente. Buitengemeentelijke overheidsorganen betrekken hun gegevens in beginsel bij de registratiehouder, het Ministerie van Binnenlandse Zaken, tenzij het niet om systematische verstrekkingen gaat.

In het geval verwerking van persoonsgegevens door verwerkers (bijvoorbeeld leveranciers) wordt uitgevoerd, in opdracht van of namens gemeentelijke overheidsorganen, is het desbetreffende gemeentelijke orgaan verantwoordelijk voor de rechtmatige verwerking.

Dan moeten verantwoordelijke en verwerker borging van verantwoordelijkheden, doelbinding, transparantie, geheimhouding, informatiebeveiliging, toezicht en naleving vastleggen in een verwerkersovereenkomst.

4.3.2 Welke gegevens worden verstrekt?

Als duidelijk is dat de gegevens uit de BRP verstrekt mogen worden, moet worden bepaald welke gegevens. Van toepassing zijn:

- De wettelijke eis dat de gegevens "noodzakelijk zijn voor de uitvoering van hun taken";
- Er worden niet meer gegevens geleverd dan noodzakelijk voor de uitoefening van de taak.

4.3.3 Het verder verwerken van gegevens afkomstig uit de BRP

Als een afnemer gegevens afkomstig uit de BRP opslaat in een eigen applicatie, al dan niet aangevuld met eigen gegevens, dan is de wet BRP niet meer direct van toepassing. Wel moet bij een eventuele doorlevering rekening worden gehouden met de grondslagen (het doel) waarvoor de gegevens zijn verkregen. De verstrekker geeft de afnemer informatie ten aanzien van het bijzondere karakter van het verder verwerken van gegevens afkomstig uit de BRP. De verstrekker is niet de instantie die de rechtmatigheid van die verwerking toetst.

Ten aanzien van iedere verwerking van persoonsgegevens geldt een aantal algemene regels, vastgelegd in de AVG. De kern van deze wet is als volgt te omschrijven:

- Er moet een rechtmatige grondslag zijn (art. 6 AVG).

- De verwerking van persoonsgegevens is transparant.
- Er is sprake van doelbinding (art. 5 lid 1 AVG).
- Er wordt voldaan aan bepaalde kwaliteitsvereisten.
- De rechten van betrokkenen worden gerespecteerd.
- De gegevens zijn voldoende beveiligd.

4.4 Adviesverzoek aan de privacy officer

De privacy officer geeft advies over de gewenste verwerking van persoonsgegevens. De privacy officer weegt de bij de verwerking betrokken belangen (bijvoorbeeld; dienstverlening of fraudebestrijding) af tegen de inbreuk op de privacy van betrokkenen. Bij een geautomatiseerde verstrekking uit de BRP is de verstrekker verplicht de privacy officer om advies te vragen. De privacy officer geeft niet alleen advies ten aanzien van verstrekkingen uit de BRP. Ook andere verwerkingen van persoonsgegevens, waaronder doorleveren, behoren te worden voorgelegd aan de privacy officer.

Het advies van de privacy officer is niet bindend. Uitgangspunt is dat het advies wordt opgevolgd.

Slechts bij zwaarwegende argumenten kan hiervan worden afgeweken.

Het advies wordt opgenomen in het dossier in het zaakstelsel.

4.5 Functionaris Gegevensbescherming en rol privacy officer

De FG houdt toezicht op de toepassing en naleving van de AVG. De FG informeert en adviseert de verantwoordelijke of de verwerker over hun verplichtingen uit hoofde van de AVG en andere gegevensbeschermingsbepalingen.

De afnemende partij voert een Baselinetoets en/of DPIA uit. De afnemer wint in eerste instantie advies over de DPIA in bij de privacy officer. In geval van complexe gegevensverwerking zal de privacy officer de FG consulteren. Het advies van de FG wordt in de DPIA vastgelegd.

4.6 Informatiebeveiliging en verwerkersovereenkomst

Het gemeentelijk beleid ten aanzien van informatiebeveiliging is van toepassing. In de praktijk betekent dit dat aan de hand van een verkorte risicoanalyse wordt bekeken of de BIO toereikend is, of dat er op basis van de risicoanalyse extra maatregelen noodzakelijk zijn. Als dat het geval is worden deze extra maatregelen vastgesteld op basis van een uitgebreide risicoanalyse en/of een DPIA.

Voor leveringen uit de BRP is het aan de afnemer om aan te tonen dat hij voldoet aan de (gemeentelijke) richtlijnen en aan de vereisten voor aansluiting. In het geval van verwerking van persoonsgegevens door een verwerker (bijvoorbeeld een externe leverancier) is een verwerkersovereenkomst noodzakelijk. Hierin staan de afspraken tussen het gemeentelijk orgaan (verwerkingsverantwoordelijke) en de verwerker over onder andere borging van verantwoordelijkheden, doelbinding, transparantie, geheimhouding, informatiebeveiliging, toezicht en naleving van (verwerkers-) afspraken.

4.7 Belangenafweging en conflictbeheersing

Om te voorkomen dat medewerkers van verschillende teams in conflictsituaties verzeild raken is een goede systematiek voor conflictbeheersing vereist. Met het doorlopen van de voorgaande stappen moet helder zijn wat de achtergronden zijn bij de belangen die leiden tot het conflict. De vertegenwoordigde belangen kunnen hun grondslag vinden in wetgeving, politieke motieven, doelmatigheidsoverwegingen, dienstverlening, etc.

Doorgaans staan de verschillende belangen niet ter discussie, maar gaat het om het vinden van de juiste balans. Als er zich toch een conflict voordoet leggen uitvoerende medewerkers een belangenconflict in eerste instantie voor aan de verantwoordelijke managers. Deze managers proberen onderling tot een oplossing te komen. Voor strikt juridische conflicten kan de casus voorgelegd worden aan het team Juridische Zaken van de Bedrijfsvoeringsorganisatie West-Betuwe. Juridische zaken geeft haar oordeel in de vorm van een advies aan de managers van de verzoekende teams. Conflicten op het vlak van gegevensbeveiliging kunnen worden voorgelegd aan de CISO. De CISO geeft een oordeel in de vorm van een advies aan de betrokken managers. Als de FG en de CISO conflicterende adviezen of verschillen van inzicht hebben, wordt het conceptbesluit over de gegevensverwerking voorgelegd aan het college.

4.8 Besluit tot verstrekking en aansluiting op de BRP

De verstrekker neemt namens B en W een formeel besluit tot verstrekking van gegevens uit de BRP.

Dit besluit wordt verzonden naar de afnemer.

Technische realisatie wordt door de verzoekende partij afgestemd met de verstrekker.

Uitgangspunt hierbij is dat zoveel mogelijk gebruik gemaakt wordt van de beschikbare gemeentelijke standaarden en richtlijnen.

Projectmanagement maakt beperkt gebruik van het changeproces. Technische realisatie van aansluiting op het gegevensmagazijn wordt binnen het project uitgevoerd.

4.9 Controle op de rechtmatige verwerking van persoonsgegevens afkomstig uit de BRP

De afnemer heeft de verantwoordelijkheid voor het waarborgen van de transparantie van de verwerking van persoonsgegevens uit de BRP. De verstrekker controleert periodiek de rechtmatige verwerking van persoonsgegevens afkomstig uit de BRP. De afnemer is verplicht om aan deze controle mee te werken. Als onregelmatigheden worden gesignaleerd zal de verstrekker dit bespreken met de afnemer. Als de problemen niet opgelost (kunnen) worden zal de verstrekker dit op bestuurlijk niveau aankaarten.