Gemeente Brummen

GEMEENTEBLAD

Officiële uitgave van de gemeente Brummen

Nr. 46092

20 februari 2020

BEVELIGINGSRICHTLIJN BASISREGISTRATIE PERSONEN GEMEENTE BRUMMEN

Kenmerk Z041084 / D320943

HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN DE GEMEENTE BRUMMEN,

Hebben besloten:

1. De beveiligingsrichtlijn Basisregistratie Personen en de Regeling beheer en toezicht Basisregistratie Personen vast te stellen.

Beveiligingsrichtlijn Basisregistratie Personen

Algemeen

De beveiligingsrichtlijn Basisregistratie Personen (Beveiligingsrichtlijn BRP) is een aanvulling op het algemene informatiebeveiligingsbeleid en geeft invulling aan specifieke eisen ten aanzien van het vakgebied. Het college van burgemeester en wethouders stelt in verband met de beveiliging van de Basisregistratie Personen (BRP) de beveiligingsrichtlijn BRP vast.
De wetgever stelt in de Wet Basisregistratie Personen (BRP) eisen aan de beveiliging van de uitvoeringsprocessen voor de BRP. Het verantwoordelijke bestuursorgaan voor de BRP is het college van burgemeester en wethouders. Het verantwoordelijke bestuursorgaan dient jaarlijks te rapporteren over de mate waarin en de wijze waarop wettelijke regelgeving wordt gehandhaafd. Aan de getroffen beveiligingsmaatregelen dient een richtlijn aangaande informatiebeveiliging ten grondslag te liggen. De uitgangspunten en beveiligingsprocedures die invulling aan de gestelde eisen moeten geven zijn in deze richtlijn opgenomen. Dit document maakt onderdeel uit van het opgestelde Informatiebeveiligingsbeleid en vormt de basis voor de uit te voeren procedures.
Op grond van artikel 4.3 van de Wet BRP dient het informatiebeveilingsbeleid BRP operationeel te zijn. De beveiligingsrichtlijn BRP wordt operationeel door het benoemen van medewerkers die belast zijn met onderscheidende, uitvoerende, en controlerende taken, evenals het beschrijven van de meest fundamentele werkprocedures binnen dit kader. Deze zijn vastgelegd in de Regeling beheer en toezicht BRP, respectievelijk het Handboek procedures Basisregistratie Personen.

Inleiding

Op basis van de Algemene Verordening Gegevensbescherming (AVG) is de gemeente Brummen verplicht tot het verzorgen van beveiligingsmaatregelen rondom de verwerking van persoonsgegevens in alle bedrijfsprocessen. De gemeentelijke BRP processen zijn niet de enige processen waarvoor tevens in wetten of reglementen staat voorgeschreven, dat het treffen van beveiligingsmaatregelen noodzakelijk is. De gemeente verwerkt persoonsgegevens ook binnen tal van andere processen, waarbij evengoed wettelijke regels kunnen gelden.
Het gemeentebrede “Informatiebeveiligingsbeleid gemeente Brummen” bevat kaders en richtlijnen voor informatiebeveiliging, noodzakelijk om de totale bedrijfsvoering van de gemeente Brummen te beveiligen. De beveiligingsrichtlijn BRP is een aanvulling op het gemeentebrede informatie-beveiligingsbeleid, maar is voor wat betreft algemene beveiligingsmaatregelen afgestemd op de inhoud van de voor gemeenten, provincies, waterschappen en Rijk vastgestelde Baseline Informatiebeveiliging Overheid (BIO).
De Wet Basisregistratie Personen (Wet BRP) is de grondslag voor de basisregistratie persoons-gegevens en vervangt de Wet Gemeentelijke Basisadministratie persoonsgegevens (Wet GBA). De Wet BRP schrijft vernieuwing van de ICT-infrastructuur voor, waardoor het op termijn mogelijk moet worden om plaats onafhankelijke dienstverlening aan burgers te kunnen verlenen. Sommige door de Wet BRP voorgeschreven wijzigingen kunnen pas worden doorgevoerd als voorgestelde nieuwe ICT-voorzieningen in gebruik zijn genomen. Het realiseren van de nieuwe ICT-voorzieningen gebeurde aan de hand van het programma “Operatie BRP”. Op 5 juli 2017 heeft de Minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) besloten om de Operatie BRP ordentelijk af te bouwen en te beëindigen. Totdat nieuwe ICT-voorzieningen zijn opgeleverd, blijven gemeenten (gedeeltelijk) de ICT-voorzieningen van de GBA gebruiken. Deze oude voorziening wordt aangeduid als ‘gemeentelijke voorziening’.

Totstandkoming, implementatie en evaluatie

Totstandkoming

Ten behoeve van de totstandkoming van de beveiligingsrichtlijn BRP, is er periodiek overleg tussen de privacybeheerder BRP, de beveiligingsbeheerder BRP en de informatiebeheerder BRP. De aanwijzing van deze functionarissen en de omschrijving van hun specifieke taken binnen het informatiebeveiligingsbeleid BRP zijn opgenomen in de Regeling beheer en toezicht Basisregistratie Personen. De leden van deze overleggroep hebben een sleutelrol in het beheer van de gemeentelijke voorziening.

Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als dit op een gestructureerde manier wordt georganiseerd en de betrokken actoren de hun toegewezen taken op correcte wijze uitvoeren. Beleidsdoelstellingen zijn bepalend voor de invulling van het informatiebeveiligingsbeleid en in de Beveiligingsrichtlijn BRP zijn deze doelstellingen specifiek gericht op de BRP. Medewerkers moeten (o.a. tijdens werkoverleggen) bij de implementatie en ontwikkeling van het opgestelde beleid worden betrokken en zijn mede verantwoordelijk voor de uitvoering van het beleid. Op basis van hun rollen en taken binnen de organisatie worden verantwoordelijkheden aan hen toegewezen. De controller informatiebeveiliging heeft hierbij als taak om vast te stellen of er bij de uitvoering van deze taken sprake is van het naleven van de opgestelde procedures.

De beveiligingsrichtlijn BRP bevat een stelsel van procedures en maatregelen die bestemd zijn voor toepassing in de dagelijkse praktijk. De betreffende procedures op het gebied van de BRP moeten periodiek worden bezien op actualiteit. In deze richtlijn zijn daarom duidelijke afspraken vastgelegd over de verantwoordelijkheid voor de handhaving en naleving van getroffen maatregelen en procedures.

De beveiligingsrichtlijn BRP wordt jaarlijks geëvalueerd door de beveiligingsbeheerder, in overleg met de privacybeheerder en de informatiebeheerder. De beveiligingsbeheerder controleert ook of de bij de richtlijn opgenomen procedures nog steeds relevant en actueel zijn en stelt deze indien nodig bij. De gewijzigde procedures worden vastgesteld door de procesmanager Inwonerszaken.

De gewijzigde richtlijn wordt, met de vastgestelde procedures, ter kennisgeving aangeboden aan het OT en wordt vervolgens ter vaststelling aangeboden aan het college van burgemeester en wethouders.

Alle medewerkers van de gemeente Brummen worden via de gebruikelijke interne kanalen geïnformeerd over wijzigingen binnen de beveiligingsrichtlijn en aanpassingen binnen maatregelen of procedures over informatiebeveiliging. Indien nodig kan dit ook via het reguliere werkoverleg plaatsvinden.

Het gehele beleid dient minimaal eenmaal per raadsperiode te worden herijkt.

Beleidsuitgangspunten

Informatiebeveiliging

De Baseline Informatiebeveiliging Overheid (BIO) vormt het normenkader waaraan de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van gemeentelijke informatie(systemen) dient te voldoen. De BIO is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat dat voor iedere overheid in Nederland geldt. Voor specifieke maatregelen is in onderhavige BIO ook gebruik gemaakt van onder andere de AVG, de SUWI-wet, BRP, BAG en PUN.

De beveiligingsrichtlijn BRP is afgestemd op de inhoud van de BIO, en is daarnaast gebaseerd op regelgeving zoals die vermeld wordt in de in de aparte hoofdstukken van dit plan.

Beleidsdoelstelling

Het gemeentebestuur van de gemeente Brummen neemt zich ten aanzien van de informatiebeveiliging voor, om beveiligingsmaatregelen te treffen die de continuïteit van de bedrijfsvoering moeten garanderen. De getroffen maatregelen vallen uiteen in fysieke, organisatorische en logische maatregelen. De verschillende soorten maatregelen richten zich in ieder geval op beschikbaarheid, integriteit, vertrouwelijkheid van gegevens en de controleerbaarheid van de gemeentelijke bedrijfsprocessen. Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het gemeentebestuur van de gemeente Brummen de uiteindelijke verantwoordelijkheid draagt. Op het gebied van de BRP en waardedocumenten neemt zij daarbij de algemene en specifieke eisen van het wettelijk kader als uitgangspunt.

Wettelijk kader verwerking persoonsgegevens

De AVG vormt het algemeen kader voor de verwerking van persoonsgegevens. De AVG stelt dat overheden hiervoor passende technische en organisatorische maatregelen moet nemen.

Buiten het algemeen kader van de AVG dient het gemeentebestuur ook rekening te houden met de beveiligingseisen die andere wetten stellen. Voor de beveiligingsrichtlijn BRP is dat de Wet BRP.

De autoriteit Persoonsgegevens (AP) kan de verantwoordelijke voor de verwerking van persoonsgegevens in de BRP, het college van burgemeester en wethouders, aanspreken op het niveau van de maatregelen voor de beveiliging van de verwerking van persoonsgegevens en de wijze waarop het stelsel van maatregelen is geïmplementeerd en wordt nageleefd.

Taken, verantwoordelijkheden en bevoegdheden

De bestuurlijke verantwoordelijkheid voor de beveiligingsrichtlijn BRP ligt bij het college van B en W. Beveiliging op ambtelijk niveau betreft de verantwoordelijkheid van alle leden van het Ondersteuningsteam (OT). Het OT bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

De informatiebeheerder is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid op het gebied van de persoonsinformatievoorziening. De informatiebeheerder is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van de beveiligingsrichtlijn BRP.
De Chief Information Security Officer (CISO) is op gemeentelijk niveauverantwoordelijk voor de informatiebeveiliging. De CISO is verantwoordelijk voor het opstellen en actualiseren van het gemeentebrede informatiebeveiligingsplan en het gezamenlijk met de proceseigenaren afstemmen van de beveiligingsmaatregelen op procesniveau.
De controller informatiebeveiliging is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van de beveiligingsrichtlijn BRP en ziet erop toe dat eens per jaar gecontroleerd wordt of de nog te nemen maatregelen gerealiseerd zijn. Deze rol is vastgelegd in de Regeling Beheer en Toezicht BRP.
Ook de verantwoordelijkheden van de rollen en/of functies van de gegevensbeheerder, privacybeheerder, applicatiebeheerder, systeembeheerder en beveiligingsbeheerder, zijn vastgelegd in de Regeling beheer en Toezicht BRP.

Passende technische en organisatorische maatregelen
Welk niveau van technische en organisatorische maatregelen passend is, wordt bepaald door de risicoklasse waarin de persoonsgegevens worden ingedeeld en de context waarbinnen de gegevens worden verwerkt.
De in de BRP vastgelegde persoonsgegevens zijn op grond van de door de Autoriteit Persoonsgegevens (AP) gehanteerde classificatie ingedeeld in risicoklasse II (verhoogd risico). Dat wil zeggen er bestaan in vergelijking met het basisniveau van risicoklasse I extra negatieve gevolgen voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De indeling in deze risicoklasse komt voort uit de aard van de gegevensverwerking in de BRP: de gegevens die worden verwerkt hebben betrekking op de gehele bevolking van de gemeente Brummen.
De BRP is conform de classificatiematrix van de Baseline Informatiebeveiliging Overheid (BIO) ingedeeld in de categorie “hoog” op de aspecten vertrouwelijkheid, integriteit en beschikbaarheid. De maatregelen die worden getroffen dienen in lijn te zijn met dit classificatieniveau.
Een passend beveiligingsniveau
Een adequaat niveau van beveiliging van persoonsgegevens kan worden bereikt door het treffen van een stelsel van technische en organisatorische maatregelen, waarvan het niveau aansluit bij de risico’s welke verbonden zijn aan de gedefinieerde risicoklasse.
Kwaliteitsaspecten
Het Informatiebeveiligingsbeleid omvat een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijke top eendrachtig duidelijk maken aan het tactisch en operationeel niveau welke gedragslijn de gemeente Brummen dient te volgen om te komen tot een adequate informatiebeveiliging.
Het maken en vaststellen van beveiligingsbeleid biedt nog geen garantie voor een goede werking. Hiervoor is het nodig dat de uitgangspunten in het Informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het directieteam vast te stellen of de maatregelen werken. Evaluatie van het beleid dient vervolgens plaats te vinden om na te gaan of het beleid nog steeds aansluit op de organisatie en of de juiste maatregelen zijn getroffen.
De beveiliging van persoonsgegevens kent vier kwaliteitsaspecten, namelijk:
1: **Beschikbaarheid**. De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn in overeenstemming met de daarover gemaakte afspraken en de wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.
2: **Integriteit**. De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
3: **Vertrouwelijkheid**. Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.
4: **Controleerbaarheid**. Een regelmatige controle op uitvoering van de beheermaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trails) van groot belang. Controleerbaarheid is de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd en gebruikt.
De gemeente Brummen hanteert voor deze kwaliteitsaspecten de volgende normen:
Norm voor beschikbaarheid
Het college van B en W en het directieteam zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te staan als de informatievoorziening wordt gestaakt en een aantal bedrijf kritische applicaties niet meer functioneren. Dit geldt onder andere en in het bijzonder voor de informatievoorziening vanuit de BRP. Het functioneren van de BRP is cruciaal tijdens de openingstijden voor het publiek.
Voor de continuïteit van de bedrijfsvoering is het noodzakelijk dat de gemeente voorzieningen treft, die onverhoopte storingen binnen het landelijke systeem kunnen opvangen. Dit betreft voorzieningen die betrekking hebben op de gegevensbestanden, netwerkverbindingen en lokale systemen.

De eerstkomende jaren zal de BRP nog worden uitgevoerd met behulp van de lokale voorzieningen die gebaseerd zijn op de Wet GBA. Voor deze voorzieningen geldt dat een uitval nooit langer mag duren dan 48 uur. Er dienen adequate voorzieningen te zijn getroffen om ook in geval van calamiteiten, na maximaal 48 uur de dienstverlening aan de burger en aan andere bestuursorganen te kunnen hervatten.
Norm voor integriteit
De technische en organisatorische inrichting van de gemeentelijke informatiesystemen zijn zodanig van aard en opzet, dat de gegevens daarbinnen volledig, juist, en actueel zijn. De verantwoordelijke personen en afdelingen binnen de gemeentelijke organisatie treffen de benodigde maatregelen om dit zeker te stellen.
Het is niet te voorkomen dat gegevens fouten bevatten. Een BRP-bestand zonder fouten is een nobel streven, maar het is niet realistisch om dit als concrete eis te stellen. Ten behoeve van het evaluatie instrument zijn kwaliteitsindicatoren opgesteld over de gegevens die in de BRP zijn opgenomen. Deze indicatoren zijn gebaseerd op het Logisch Ontwerp en op geldende regelgeving.
Aan de hand van kwaliteitsindicatoren wordt bepaald in hoeverre de vastgelegde gegevens voldoen aan de vastgestelde eisen. De kwaliteitsindicatoren meten niet de overeenstemming van de BRP-gegevens met de 'feitelijke werkelijkheid'.
Bij de uitgangspunten voor de beoordeling van de kwaliteitsindicatoren wordt onderscheid gemaakt tussen zes klassen:

Klasse	Omschrijving	Norm (2019)
A	Persoon en Overlijden Groep 1, 1e en 6e	99,7 %
B	Adres Groep 1, 6e	99,7 %
C	Relaties Groep 1, 1e	99,6 %
D	Identificatienummers en nationaliteit Groep 2, 7e Groep 2, 4e Groep 2, 8e	99,5 %
E	Overig algemeen Groep 2, 9e Groep 2, 5e Groep 2, 2e en 3e Groep 2, 10e Groep 2, 11e	99,5 %
F	Administratief Groep 3, 1e, 2e, 3e, 4e	99,4 %

Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens hanteert de gemeente de wettelijk bepaalde normen.

Norm voor vertrouwelijkheid
Uitsluitend bevoegde personen in dienst van of werkzaam ten behoeve van de gemeente Brummen hebben toegang tot en kunnen bij de uitvoer van hun taken gebruik maken van de in de voor hen relevante registraties opgenomen gegevens. De bevoegdheid van een persoon moet worden afgeleid van diens taak, dit ter beoordeling van de procesmanager. Diegenen van de voornoemde personen, die belast zijn met de registratie van BRP gegevens dienen een geheimhoudingsverklaring te hebben ondertekend.
Norm voor controleerbaarheid
Mutaties van persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente reiken. Toelating tot Nederland is bijvoorbeeld mede afhankelijk van de nationaliteit van de aanvrager. Hoogte en duur van uitkeringen zijn veelal afhankelijk van leeftijd en de burgerlijke staat. Dat betekent niet alleen dat de kwaliteit van de geregistreerde gegevens hoog dient te zijn, maar lettend op mogelijke belangenverstrengeling dient er ook gecontroleerd te kunnen worden wie welke mutatie heeft verwerkt en wie welke raadplegingen heeft gedaan.
Nadere uitwerking normering
In 2020 zal voor de BRP vanuit de richtlijnen van de BIO een risicoanalyse gemaakt worden, waarbij op basis van de hierboven genoemde normen voor beschikbaarheid en controleerbaarheid de noodzakelijke beveiligingsmaatregelen worden vastgesteld en geïmplementeerd. Hiermee geven we in 2020 invulling aan de wettelijke vereisten en de kaders van het informatiebeveiligingsbeleid Brummen.
Samenvatting
Beveiliging van (persoons-)gegevens vraagt om een zorgvuldige analyse van de risico's die met de gegevensverwerking samenhangen. Er zijn verschillende risico's te noemen die ertoe kunnen leiden dat bedrijfsprocessen stagneren. Bijvoorbeeld verlies van gegevens (raakt aan de kwaliteitsaspecten integriteit en beschikbaarheid) en onrechtmatig gebruik van gegevens (raakt aan het aspect vertrouwelijkheid), maken de resultaten van bedrijfsprocessen onbetrouwbaar. De in het voorliggende plan Informatiebeveiliging BRP en waardedocumenten opgenomen procedures hebben als doel te voorkomen, dat de risico's uit de aan verwerking van persoonsgegevens verbonden risicoklasse (II)

Wbp zich voordoen. Uitvoering van de procedures maakt het bedrijfsproces controleerbaar uit oogpunt van beveiliging.

Basisregistratie Personen (BRP)
Wettelijk kader
Het op schrift stellen van de - in de praktijk van alledag al ingeburgerde - beveiligingsprocedures is noodzakelijk om objectief te kunnen bepalen of de BRP-bestanden en bepaalde processen voldoen aan de eisen ten aanzien van beschikbaarheid (continuïteit), integriteit (betrouwbaarheid), vertrouwelijkheid (exclusiviteit) en controleerbaarheid.
De gemeente moet op grond van de AVG en de Wet BRP de beveiligingsmaatregelen nemen die de wet voorschrijft. Als grondslag voor het beveiligingsbeleid op het onderdeel BRP zijn van belang de artikelen 1.10 en 1.11 Wet BRP. Artikel 1.10 bepaalt dat de beveiligingsmaatregelen BRP bij of krachtens Algemene Maatregel van Bestuur (AMvB) worden geregeld (het Besluit BRP). Artikel 1.11 draagt het college van B&W op zich aan die maatregelen te houden. Daarnaast is artikel 32 van de AVG van toepassing.
Bovendien geldt op grond van artikel 4.3 Wet BRP de verplichting om jaarlijks uiterlijk op 31 december zelf onderzoek te doen naar de inrichting, de werking en de beveiliging van de basisregistratie, evenals naar de verwerking van gegevens in de basisregistratie.
Gelet op het belang voor het beveiligingsbeleid volgen hieronder de teksten van artikel 6 Besluit BRP en van artikel 32 AVG.

Artikel 6 Besluit BRP
1. Het college van burgemeester en wethouders treft ten aanzien van de gemeentelijke voorziening passende technische en organisatorische maatregelen ter beveiliging van de in de basisregistratie opgenomen gegevens tegen verlies of aantasting van deze gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking van deze gegevens.
2. Onze Minister treft ten aanzien van de centrale voorzieningen passende technische en organisatorische maatregelen ter beveiliging van de in de basisregistratie opgenomen gegevens tegen verlies of aantasting van deze gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking van deze gegevens.
3. De in het eerste en tweede lid bedoelde maatregelen omvatten ten minste:
a. maatregelen gericht op personen die werkzaam zijn voor de verantwoordelijke voor de verwerking van gegevens in de basisregistratie;
b. maatregelen gericht op de toegang tot gebouwen en ruimten waar in de basisregistratie opgenomen gegevens aanwezig zijn;
c. maatregelen gericht op een deugdelijke werking en beveiliging van de apparatuur en programmatuur;
d. maatregelen voor het geval de geheimhouding of integriteit van in de basisregistratie opgenomen gegevens is geschaad;
e. maatregelen bij calamiteiten.

Artikel 32 AVG
1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.
4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.
Periodieke zelfevaluatie

De in de beveiligingsrichtlijn voorgestelde beveiligingsmaatregelen en –procedures vormen voor eens per jaar het object van onderzoek, bij de door Wet BRP voorgeschreven zelfevaluatie BRP. De uitslagen van deze zelfevaluatie wordt door het college van B&W naar de Rijksdienst Identiteitsgegevens gezonden en openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. De Kwaliteitsmonitor is ook voor de controle op de inhoudelijke kwaliteit van de gegevens.
Onderzoek BRP gegevens
De Rijksdienst voor Identiteitsgegevens voert periodiek inhoudelijke kwaliteitscontroles uit op de gegevens in de landelijke voorziening voor de BRP en stelt de resultaten van die controles beschikbaar via de Kwaliteitsmonitor. Elke gemeente kan de resultaten van het op haar betrekking hebbende onderdeel van de BRP in het onderdeel 'monitor gegevens' van de Kwaliteitsmonitor bekijken met behulp van een persoonlijke login. De gegevens in de BRP moeten voldoen aan de kwaliteitsnormen, welke op grond van artikel 47 Besluit BRP bij ministeriële regeling worden bepaald.
Naast de kwaliteitscontroles van de Rijksdienst voor Identiteitsgegevens voert de gegevensbeheerder BRP ook controlewerkzaamheden uit ter waarborging van de kwaliteit van de gegevens in de BRP. Dit is beschreven in de Regeling beheer en Toezicht BRP en in de procedures in het Handboek Informatieprocedures BRP.
Onderzoek BRP processen
Gemeenten moeten periodiek zelf onderzoeken of zij voldoen aan de eisen die de wetgever stelt op het gebied van beveiliging en privacy bij de uitvoering van de BRP-werkzaamheden. Deze controle voert de gemeente uit aan de hand van een digitale vragenlijst BRP die de Rijksdienst Identiteitsgegevens via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt. De vragenlijst moet jaarlijks vóór 31 december definitief zijn ingevuld. De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de gemeentecontroller en voorzien van een actieplan van de gemeente) ter kennisgeving aan het college van B en W worden gestuurd. Deze ondertekent de rapportage en stuurt deze vóór 14 februari aan de Rijksdienst voor Identiteitsgegevens toe.

Inwerkingtreding
Deze regeling treedt inwerking met ingang van de dag na de dag van bekendmaking.

Citeertitel
Deze regeling kan worden aangehaald als: beveiligingsrichtlijn Basisregistratie Personen.

Dit besluit is genomen tijdens de vergadering van het College van Burgemeester en Wethouders van 11 februari 2020.
Het college B&W van de gemeente Brummen,
Burgemeester A.J. van Hedel