

Informatiebeveiligingsplan BRP en Waardedocumenten 2017

INLEIDING

De wetgever stelt in de Wet basisregistratie personen (BRP), de Paspoortwet en het Reglement Rijbewijzen eisen aan de beveiliging van de uitvoeringsprocessen voor de BRP en Waardedocumenten. De verantwoordelijke bestuursorganen, burgemeester en wethouders voor de BRP respectievelijk de burgemeester voor de andere twee processen, moeten jaarlijks rapporteren in hoeverre de organisatie aan deze eisen voldoet. Aan de beveiliging dient een Informatiebeveiligingsplan ten grondslag te liggen, waarin de uitgangspunten en beveiligingsprocedures zijn opgenomen die invulling geven aan die eisen. Het beveiligingsbeleid en de beveiligingsprocedures voor de BRP en Waardedocumenten die voor de gemeente Molenwaard van toepassing zijn, worden in dit document beschreven en vormt de basis voor de uit te voeren procedures en controles waarover jaarlijks wordt gerapporteerd en waarnaar wordt verwezen in het hoofdstuk bijlagen.

Dit informatiebeveiligingsplan beschrijft op tactisch niveau de maatregelen die door de gemeente Molenwaard dienen te worden genomen op het gebied van informatiebeveiliging ten aanzien van de Wet basisregistratie personen (BRP) en Waardedocumenten. Het plan moet gezien worden als een specifieke aanvulling op het Strategisch informatiebeveiligingsbeleid van de gemeente Molenwaard en het tactisch Informatiebeveiligingsjaarplan gemeente Molenwaard 2015-2016, waarin het gemeentebrede beveiligingsbeleid is omschreven om de totale bedrijfsvoering van de gemeente Molenwaard te beveiligen. Alle drie genoemde documenten worden door het college van burgemeester en wethouders vastgesteld.

De Wet basisregistratie personen (Wet BRP) is de nieuwe grondslag voor de basisregistratie van persoonsgegevens en heeft de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA) vervangen. De Wet BRP maakt onder andere vernieuwing van de ICT mogelijk en hierdoor wordt op termijn plaatsafhankelijke dienstverlening voor burgers geïntroduceerd. Sommige van de wijzigingen kunnen pas worden doorgevoerd als de nieuwe ICT-voorzieningen (bijvoorbeeld BRP-ICT) in gebruik worden genomen. Deze worden gerealiseerd door het landelijke programma modernisering GBA. Totdat alle nieuwe ICT-voorzieningen zijn opgeleverd, blijven gemeenten (gedeeltelijk) de GBA-ICT gebruiken, deze worden aangeduid als 'gemeentelijke voorziening.'

ORGANISATIE VAN DE INFORMATIEBEVEILIGING

Totstandkoming van dit plan

In de gemeente Molenwaard is voor de totstandkoming van dit specifieke Informatiebeveiligingsplan BRP en Waardedocumenten een interne overleggroep informatiebeveiliging BRP en Waardedocumenten ingesteld. De samenstelling van deze groep bestaat uit het afdelingshoofd Klant Contact (tevens informatiebeheerder BRP), de teamleider Burgerzaken, de applicatiebeheerder/gegevensbeheerder en de privacybeheerder.

De leden van de overleggroep informatiebeveiliging hebben of een sleutelrol in het beheer van de gemeentelijke voorziening, of in het beheer van Waardedocumenten, of in de (fysieke) beveiliging van de backoffice en het personeel.

Over de inhoud van dit specifieke informatiebeveiligingsplan voor de BRP en Waardedocumenten vindt intensieve afstemming plaats met de Chief Information Security Officer (CISO).

Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt en alle factoren die daarbij een rol hebben, daar op een juiste manier invulling aan geven. Binnen de organisatie moeten medewerkers verantwoordelijkheden krijgen voor de implementatie van dit beleid.

De medewerkers worden betrokken (o.a. tijdens werkoverleg) bij de ontwikkeling en implementatie van het beleid en zijn mede verantwoordelijk voor de uitvoering. Daarnaast moet door de controller informatiebeveiliging worden vastgesteld of de maatregelen worden nageleefd.

Dit plan wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de beveiligingsbeheerder en bij noodzaak daartoe bijgesteld. Alle medewerkers van de gemeente Molenwaard worden via de gebruikelijke interne kanalen en voor zover noodzakelijk door hun leidinggevende via het reguliere werkoverleg geïnformeerd over voor hen van belang zijnde wijzigingen in het specifieke informatiebeveiligingsbeleid, -plan, -maatregelen en/of -procedures voor de BRP en Waardedocumenten.

Alle wijzigingen die direct betrekking hebben op individuele taken en bevoegdheden worden expliciet door de leidinggevende met zijn of haar betrokken medewerker(s) rechtstreeks gecommuniceerd.

Dit Informatiebeveiligingsplan BRP en Waardedocumenten bevat tevens een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden gezien op actualiteit. In dit plan zijn daarom afspraken vastgelegd over de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen en procedures met betrekking tot BRP en Waardedocumenten. De belangrijkste afspraak in dit verband is dat de overleggroep informatiebeveiliging het voorliggend Informatiebeveiligingsplan BRP en Waardedocumenten en de daarbij behorende procedures en bijlagen jaarlijks opnieuw bekijkt op actualiteit en controleert op naleving van de beleidsuitgangspunten.

De overleggroep informatiebeveiliging biedt het aangepaste plan vervolgens rechtstreeks ter advisering aan de gemeentesecretaris en het managementteam aan. Daarna wordt het ter vaststelling aangeboden aan de bevoegde bestuursorganen, het college van B&W respectievelijk de burgemeester.

Verantwoording

De Baseline Informatiebeveiliging Gemeenten (BIG) is het normenkader dat de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van gemeentelijke informatie(systemen) bevordert. Deze Baseline is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. Deze Baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2007 en NEN/ISO 27001:2005. Deze standaard is voor de Nederlandse Overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Voor specifieke maatregelen is in onderhavige Baseline ook gebruik gemaakt van onder andere de WBP, SUWI-wet, BRP, BAG en PUN.

Net zoals het strategisch informatiebeveiligingsbeleid en het tactisch informatiebeveiligingsjaarplan 2015-2016 is dit specifieke Informatiebeveiligingsplan BRP en Waardedocumenten afgestemd op de inhoud van de Baseline Informatiebeveiliging Gemeenten (BIG) van KING.

Daarnaast is het voorliggend Informatiebeveiligingsplan BRP en Waardedocumenten gebaseerd op regelgeving zoals die vermeld wordt in de aparte hoofdstukken van dit plan.

Goedkeuring

Goedkeuring van de inhoud van dit document en de daarbij behorende procedures vindt plaats nadat de betrokken medewerkers van zowel de opdrachtnemer als opdrachtgever overeenstemming hebben bereikt over wat in het Informatiebeveiligingsplan BRP en Waardedocumenten staat beschreven.

Voor accordering van het voorliggend Informatiebeveiligingsplan BRP en Waardedocumenten tekent hieronder de opdrachtgever:

SPECIFIEK INFORMATIEBEVEILIGINGSBELEID BRP EN WAARDEDOCUMENTEN

Beleidsdoelstelling Molenwaard

Het gemeentebestuur van Molenwaard stelt zich ten aanzien van de informatiebeveiliging als doel om beveiligingsmaatregelen te treffen die de continuïteit van de bedrijfsvoering garanderen. Maatregelen kunnen bestaan uit fysieke, organisatorische en logische maatregelen. De verschillende soorten van 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 Molenwaard de uiteindelijke verantwoordelijkheid draagt. Het strategisch informatiebeveiligingsplan en het tactisch Informatiebeveiligingsjaarplan zijn de documenten waarin de generieke visie, doelstellingen, maatregelen etc. voor de bedrijfsvoering van de gemeente Molenwaard zijn omschreven.

Op het gebied van de BRP en Waardedocumenten neemt de gemeente Molenwaard daarbij ook de algemene en specifieke eisen van het wettelijk kader als uitgangspunt. Als concrete norm voor de realisering van de beleidsdoelstelling wordt de eis neergelegd dat de informatiesystemen aangeduid in dit specifieke Informatiebeveiligingsplan BRP en Waardedocumenten een beschikbaarheid tijdens werktijd kennen van minimaal 98%. Buiten werktijd worden er geen eisen gesteld aan de beschikbaarheid met uitzondering van voorzieningen in het kader van rampenbestrijding.

Wettelijk kader verwerking persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) vormt het algemeen kader voor de verwerking van persoonsgegevens. De verplichting tot beveiliging van persoonsgegevens is geregeld in artikel 13 van de Wbp. De tekst van dit artikel luidt:

Artikel 13 Wbp

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoer-

legging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Het College bescherming persoonsgegevens (Cbp) kan de verantwoordelijke voor de verwerking van persoonsgegevens, bij gemeenten doorgaans het college van B&W of de burgemeester, 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.

Buiten het algemeen kader van de Wbp dient het gemeentebestuur ook rekening te houden met de beveiligingseisen die andere wetten stellen, zoals dat voor dit plan zijn de Wet BRP, de Paspoortwet en het Reglement rijbewijzen. Voor dit plan is relevant dat de Wbp, voor wat betreft de verwerking van persoonsgegevens in de BRP niet van toepassing is (artikel 2, lid 2 d Wbp). De beveiliging van de BRP is geregeld bij en krachtens de Wet BRP.

Taken, verantwoordelijkheden en bevoegdheden

De bestuurlijke verantwoordelijkheid voor het Informatiebeveiligingsplan BRP en Waardedocumenten ligt bij het college van B&W respectievelijk de burgemeester. Deze organen laten het Informatiebeveiligingsplan BRP en Waardedocumenten opstellen en zien toe op de uitvoering ervan door de betreffende medewerkers.

De beveiligingsbeheerder is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid op het gebied van de persoonsinformatievoorziening.

De beveiligingsbeheerder is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van het Informatiebeveiligingsplan voor de gemeentelijke voorzieningen waarmee de gemeente Molenwaard uitvoering geeft aan de Wet BRP en voor het gegevensmagazijn.

De Chief Information Security Officer (CISO) is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van het Informatiebeveiligingsplan BRP en Waardedocumenten en ziet erop toe dat eens per jaar gecontroleerd wordt of de nog te nemen maatregelen gerealiseerd zijn (zie Regeling Beheer en Toezicht BRP).

2.3.1 Verantwoordelijkheden gemeentebestuur

Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Molenwaard. Het college van B&W stelt dit Informatiebeveiligingsplan BRP vast en de burgemeester het onderdeel Waardedocumenten.

Genoemde bestuursorganen onderschrijven volledig de beveiligingsmaatregelen die in dit Informatiebeveiligingsplan BRP en Waardedocumenten worden voorgeschreven en stellen, mede gelet op de wettelijke verplichtingen in de Wet BRP en Paspoortwet, dat de stand van zaken met betrekking tot de informatiebeveiliging jaarlijks wordt geëvalueerd om er zorg voor te dragen dat de informatiebeveiliging in de gemeente up-to-date blijft.

Voor alle gegevensverwerkende processen rond het beheer en uitgifte van waardedocumenten heeft de burgemeester op basis van de Paspoortwet en het Reglement Rijbewijzen de uiteindelijke verantwoordelijkheid.

Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van het Informatiebeveiligingsplan BRP en Waardedocumenten is de rol van de beveiligingsbeheerder in het leven geroepen. Deze heeft de verantwoordelijkheid om namens de bestuursorganen toe te zien op naleving van de beveiligingsmaatregelen en –procedures zoals uitgewerkt in het Informatiebeveiligingsplan BRP en Waardedocumenten en daarover aan het college van B&W respectievelijk de burgemeester te rapporteren.

De functie van de beveiligingsbeheerder moet niet verward worden met de functie van 'de beveiligingsfunctionaris reisdocumenten' noch die van 'de beveiligingsfunctionaris rijbewijzen'. Beide laatstgenoemde functies kennen zeer specifieke taken en verantwoordelijkheden op het beveiligingsgebied van enerzijds de reisdocumenten en anderzijds de rijbewijzen (zie bijlage Functies Waardedocumenten).

2.3.2 Verantwoordelijkheden van het managementteam

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle leden van het managementteam van de gemeente Molenwaard. Het managementteam bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

Per jaar zullen de volgende punten met betrekking tot beveiliging aan de orde komen:

- Voortgang realisatie beveiligingsmaatregelen als beschreven in het Informatiebeveiligingsplan BRP en Waardedocumenten en gerapporteerd door de beveiligingsbeheerder;
- Mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen;
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingsfunctionaris reisdocumenten en/of de beveiligingsfunctionaris rijbewijzen;
- Goedkeuring van initiatieven om de (informatie)beveiliging te verbeteren;
- Geven van voor een ieder zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen;
- Bevorderen van het beveiligingsbewustzijn;

- Herziening en goedkeuring beveiligingsbeleid en de toegekende verantwoordelijkheden.

2.3.3 Verantwoordelijkheden Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) is op gemeentelijk niveau verantwoordelijk voor de informatiebeveiliging. De CISO geeft functioneel leiding aan het werk van de IB-functies op lagere niveaus. De CISO is op het gebied van informatiebeveiliging een generalist, die op hoofdlijnen de verbanden tussen de verschillende bedrijfs- en beveiligingsbelangen moet kunnen leggen. De CISO bestrijkt alle objectgebieden. De CISO moet in staat zijn tegengestelde belangen met elkaar te verenigen, waarbij de adviezen van verschillende deskundigen en de belangen van het managementteam op waarde moet kunnen beoordeeld.

De CISO is verantwoordelijk voor:

- het opstellen van (generiek) strategisch informatiebeveiligingsbeleid, het tactisch Informatiebeveiligingsjaarplan en het Informatiebeveiligingsplan BRP en Waardedocumenten;
- de voortgang en realisatie beveiligingsmaatregelen zoals beschreven in het Informatiebeveiligingsjaarplan en het Informatiebeveiligingsplan BRP en Waardedocumenten;
- het actualiseren van het (generiek) strategisch informatiebeleid, het tactisch Informatiebeveiligingsjaarplan en het Informatiebeveiligingsplan BRP en Waardedocumenten;
- Afstemming met beveiligingsbeheerders op afdelingsniveau, waaronder de beveiligingsbeheerder en de beveiligingsfunctionaris Reisdocumenten en rijbewijzen.

De CISO rapporteert rechtstreeks aan de gemeentesecretaris.

De CISO bevordert en adviseert gevraagd en ongevraagd over de informatiebeveiliging van de gemeente Molenwaard. Ook verzorgt de CISO de rapportages over de status en kijkt of de genomen maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente Molenwaard.

2.3.4 Verantwoordelijkheden van overige rollen / functies

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.

Voor alle in dit Informatiebeveiligingsplan BRP en Waardedocumenten voorkomende functies is in de bijlage Functieverdeling de vervanging vastgelegd.

2.4 Passende 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 het College bescherming persoonsgegevens (CBP) gehanteerde classificatie ingedeeld in risicoklasse II (verhoogd risico). Dat wil zeggen er is in vergelijking met het basisoniveau van risicoklasse I extra negatieve gevolgen bestaan 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 Molenwaard.

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.

De te nemen maatregelen worden gewogen aan de hand van de volgende criteria:

- Risico's zowel van de verwerking, als ook van de aard en de omvang van de persoonsgegevens
- Stand van de techniek
- Kosten

2.4.1 Kwaliteitsaspecten

De beveiliging van persoonsgegevens kent vier kwaliteitsaspecten, namelijk:

Beschikbaarheid

De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.

Integriteit

De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.

Vertrouwelijkheid

Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.

Controleerbaar

Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trail) van groot belang. Controleerbaarheid is de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd en gebruikt.

De gemeente Molenwaard hanteert voor deze kwaliteitsaspecten de volgende normen:

2.4.1.1 Norm voor beschikbaarheid

Het college van B&W en het managementteam zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening wordt gestaakt als gevolg waarvan een aantal bedrijfskritische applicaties niet meer kunnen functioneren. Dit geldt onder andere en in het bijzonder voor de informatievoorziening vanuit de BRP.

De informatievoorziening met betrekking tot de BRP moet tijdens de openings- en werktijden permanent beschikbaar zijn. In cijfers uitgedrukt betekent dit op jaarbasis een beschikbaarheid van gemiddeld 98%.

Het functioneren van de BRP is cruciaal tijdens de openingstijden voor het publiek. Deze zijn:

Dagdeel	Tijdstip	Locatie	Adres	Kern
Maandag 1)	10.00-12.00 uur	Hof van Ammers	Bernardstraat 15	Groot-Ammers
Dinsdag	14.00-20.00 uur	De Hooghe Boei	Vletstraat 2a	Nieuw-Lekkerland
Woensdag 1)	13.00 – 15.00 uur	Dorpshuis Ottoland	Stadhoudersplein 8	Ottoland
Woensdag	17.00 – 20.00 uur	De Veste (Brede School)	Waterlinie 2-8	Nieuwpoort
Donderdag	16.00 – 20.00 uur		Kerkstraat 8	Bleskensgraaf
Vrijdag 1)	10.00 – 12.00 uur	De Vijf Lelies	Kerkstraat 33	Streefkerk

Deze locaties zijn 1 x per 4 weken gesloten.

Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt op jaarbasis tijdens kantooruren voor 98% beschikbaar te zijn.

Met kantooruren worden hier bedoeld: van maandag tot vrijdag van 07.00 tot 19.00 uur.

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 garanderen.

2.4.1.2 Norm voor integriteit

De technische en organisatorische inrichting van de gemeentelijke informatiesystemen zijn zodanig van aard en opzet dat de gegevens daarin volledig, juist, en actueel zijn. De verantwoordelijke personen en afdelingen van de gemeentelijke organisatie treffen hiervoor de nodige maatregelen.

Het is niet te voorkomen dat gegevens fouten bevatten. Een BRP-bestand zonder fouten is een nobel streven, maar is niet realistisch als concrete eis. Voor het evaluatie-instrument zijn kwaliteitsindicatoren opgesteld voor de gegevens die in de BRP zijn opgenomen. Deze indicatoren zijn gebaseerd op het Logisch Ontwerp en op regelgeving.

Met de kwaliteitsindicatoren wordt gemeten in hoeverre de vastgelegde gegevens voldoen aan de genoemde regelgeving. De kwaliteitsindicatoren meten niet de overeenstemming van de BRP-gegevens met de 'feitelijke werkelijkheid'.

Bij de uitgangspunten voor de beoordeling van de kwaliteitsindicatoren is het onderscheid in zes klassen van belang:

Klasse

A	Persoon en Overlijdensgroep 1, 1 e en 6e
B	Adres groep 1, 6e
C	Relaties groep 1, 1e
D	Identificatienummers en nationaliteitsgroep 2, 7egroep 2, 4egroep 2, 8e

E	Overig algemeengroep 2, 9egroep 2, 5egroep 2, 2 e en 3egroep 2, 10egroep 2, 11e
F	Administratiegroep 3, 1 e, 2 e, 3 e, 4e

Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens accepteert de gemeente Molenwaard een foutenpercentage van in totaal 1%.

2.4.1.3 Norm voor vertrouwelijkheid

Uitsluitend bevoegde personen in dienst van of werkzaam ten behoeve van de gemeente hebben toegang tot en kunnen 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 beheerder van de betreffende registratie, op aangeven van de direct leidinggevende van de betreffende persoon. Degenen van vernoemde personen, die belast zijn met de bijhouding van BRP gegevens en/of werken met waardedocumenten dienen een geheimhoudingsverklaring te hebben ondertekend.

2.4.1.4 Norm voor controleerbaarheid

Mutaties in persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente Molenwaard reiken. Bijvoorbeeld toelating tot Nederland is mede afhankelijk van de nationaliteit. Hoogte en duur van uitkeringen zijn veelal afhankelijk van leeftijd en burgerlijke staat. Dat betekent niet alleen dat de kwaliteit hoog moet zijn, maar dat, gelet op mogelijke belangenverstremming, ook gecontroleerd moet kunnen worden wie welke mutatie heeft verwerkt. De gemeente Molenwaard kent als norm dat 99% van alle mutaties in persoonsgegevens herleidbaar moeten zijn tot de individuele persoon die voor de mutatieverwerking verantwoordelijk was en dat zulks geldt voor 90% van alle raadplegingen.

BRP EN WAARDEDOCUMENTEN

3.1 Wettelijk kader

3.1.1 BRP

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 Wet BRP de beveiligingsmaatregelen nemen die die wet voorschrijft. De Wbp is namelijk niet van toepassing op de gegevensverwerking in het kader van de BRP.

Als grondslag voor het beveiligingsbeleid op het onderdeel BRP in dit plan 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.

Gelet op het belang voor het beveiligingsbeleid volgt hieronder de tekst van artikel 6 Besluit BRP. Wet en Besluit BRP gaan verder in het stellen van eisen aan de beveiliging dan de Wbp. Bovendien geldt op grond van artikel 4.3 wet BRP de verplichting om jaarlijkse uiterlijk op 30 september zelf onderzoek te doen naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie.

Artikel 6 Besluit BRP

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.

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. De in het eerste en tweede lid bedoelde maatregelen omvatten ten minste:

maatregelen gericht op personen die werkzaam zijn voor de verantwoordelijke voor de verwerking van gegevens in de basisregistratie;
maatregelen gericht op de toegang tot gebouwen en ruimten waar in de basisregistratie opgenomen gegevens aanwezig zijn;

maatregelen gericht op een deugdelijke werking en beveiliging van de apparatuur en programmatuur; maatregelen voor het geval de geheimhouding of integriteit van in de basisregistratie opgenomen gegevens is geschaad; maatregelen bij calamiteiten.

3.1.2 Reisdocumenten

De wetgever stelt eisen aan de opslag, uitgifte en administratie van reisdocumenten. Deze eisen zijn neergelegd in de Paspoortuitvoeringsregeling Nederland 2001, kortweg 'PUN' genoemd. Hoofdstuk XII van deze Regeling met als onderwerp beveiliging bepaalt in artikel 90: "De met de uitvoering van de wet belaste autoriteiten treffen maatregelen om de onder hen berustende reisdocumenten, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreemding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins". Deze te treffen maatregelen worden in dit Informatiebeveiligingsplan BRP en Waardedocumenten verder uitgewerkt in concrete voorschriften op het gebied van fysieke beveiliging, back-up en herstel en enkele voorschriften over hoe te handelen in bepaalde situaties. Artikel 93 lid 1 PUN vereist daartoe organisatorische maatregelen.

3.1.3 Rijbewijzen

Het uitgifteproces van rijbewijzen komt sinds enkele jaren sterk overeen met dat van de Reisdocumenten. De artikelen 122 tot en met 130 van het Reglement Rijbewijzen hebben betrekking op de eisen aan de beveiliging rondom de uitgifte van rijbewijzen. Zo wordt geëist dat de met afgifte van rijbewijzen belaste autoriteiten zorg dragen voor een op schrift gestelde beveiligingsprocedure, met daarin in ieder geval beveiligingsvoorschriften ten aanzien van: toegang van personen tot en het beheer van rijbewijzen, de met de afgifte van rijbewijzen verband houdende materialen, apparatuur, toegangspassen en gebruikerscodes tot de apparatuur, de verantwoordelijkheden van de beveiligingsfunctionaris en de functiescheiding.

3.2 Periodieke zelfevaluatie, onderzoek en accountantscontrole

3.2.1 Zelfevaluatie

De in het Informatiebeveiligingsplan BRP en Waardedocumenten voorgestelde beveiligingsmaatregelen en –procedures vormen voor een groot deel eens per jaar het object van onderzoek bij de door de Paspoortwet en Wet BRP voorgeschreven zelfevaluaties Paspoorten en NIK en BRP.

De uitslagen van deze zelfevaluaties worden door het college van B&W voor de BRP en de burgemeester voor de Reisdocumenten naar de Rijksdienst voor Identiteitsgegevens (RvIG) gezonden en openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. Die kwaliteitsmonitor is er ook voor de controle op de inhoudelijke kwaliteit van de gegevens.

3.2.2 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 de op haar betrekking hebbende onderdeel van de BRP in het onderdeel 'monitor Gegevens' van de Kwaliteitsmonitor bekijken met behulp van een persoonlijke log-in. De gegevens in de BRP moeten voldoen aan de kwaliteitsnormen, welke op grond van artikel 47 Besluit BPR bij Ministeriële regeling worden bepaald.

3.2.3 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 voor Identiteitsgegevens via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt. De vragenlijst moet jaarlijks vóór 1 oktober definitief zijn ingevuld. De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsbeheerder en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan het college van B&W. Deze ondertekent de rapportage en stuurt deze vóór 1 november naar de Rijksdienst voor Identiteitsgegevens.

De beveiligingsbeheerder neemt kennis van zowel de resultaten van deze jaarlijkse zelfevaluatie en houdt toezicht op de te ondernemen acties op geconstateerde tekortkomingen.

3.2.4 Onderzoek Paspoorten en NIK

Sinds april 2013 gebruiken gemeenten voor haar onderzoek naar het reisdocumentenproces de vragenlijst in de Kwaliteitsmonitor van de Rijksdienst voor Identiteitsgegevens. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks vóór 1 oktober definitief zijn ingevuld.

De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsfunctionaris reisdocumenten en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan de het college van B&W. Het bestuursorgaan, de burgemeester, ondertekent de rapportage en stuurt deze vóór 1 november naar de Rijksdienst voor Identiteitsgegevens.

De beveiligingsfunctionaris reisdocumenten neemt kennis van zowel de resultaten van deze jaarlijkse zelfevaluatie en houdt toezicht op de te ondernemen acties op geconstateerde tekortkomingen.

3.2.5 Accountantscontrole Rijbewijzen

Ook de procedures rond het verstrekken van rijbewijzen zijn onderwerp van controle. Op grond van artikel 128 lid 7 van het Reglement Rijbewijzen moeten de maatregelen zoals genoemd in artikel 128 lid 1 van dit reglement jaarlijks onderdeel uitmaken van de accountantscontrole.

De bij de jaarlijkse evaluatie van het beheerproces rond Waardedocumenten (reisdocumenten en rijbewijzen) geconstateerde tekortkomingen worden schriftelijk vastgelegd en de daarop betrekking hebbende rapportages worden 5 jaar bewaard. Op de eventueel geconstateerde tekortkomingen wordt actie ondernomen.

3.3 Taken, verantwoordelijkheden en bevoegdheden

Op grond van of krachtens de wet BRP, de Paspoortwet en het Reglement Rijbewijzen dienen een aantal taken, verantwoordelijkheden en bevoegdheden te worden vastgelegd en in de organisatie belegd. Zolang de gemeente de wet BRP uitvoert met de lokale voorzieningen die de Wet GBA voorschreef, dan betreft dit de beheerrollen die betrekking hebben op het informatiebeheer, gegevensbeheer, privacybeheer, applicatiebeheer en systeembeheerder. De beheerrollen ondergaan verandering, zodra de gemeente aansluit op de BRP en de GBA-voorzieningen afsluit.

Op het gebied van de Waardedocumenten dienen te worden aangewezen een beveiligingsfunctionaris reisdocumenten, de Autorisatie Bevoegde Reisdocumenten, de beveiligingsfunctionaris rijbewijzen en de Autorisatie Bevoegde Rijbewijzen.

De beschrijving en toekenning van de rollen in het kader van de Waardedocumenten maken deel uit van de bijlagen. Voor alle in dit hoofdstuk voorkomende functies is in de bijlage Functieverdeling de vervanging vastgelegd.

3.4 Functiescheiding Waardedocumenten

Om de kans te verkleinen dat medewerkers van de afdeling Burgerzaken door kwaadwillenden worden misleid (externe fraude), of dat zij al dan niet onder druk van chantage, bedreiging of omkoping misbruik maken van hun bevoegdheden (interne fraude) is functiescheiding bij het verstrekken van waardedocumenten noodzakelijk.

Hieronder een korte uitleg van de relevante termen:

Aanvraag/verstrekking: hieronder wordt verstaan het bij de balie behandelen van een aanvraag voor een waardedocument en de beslissing daarop. Bij de aanvraag van een rijbewijs dient een aanvraagformulier te worden ingevuld; bij de aanvraag van een reisdocument moet een foto- en handtekeningformulier worden gebruikt. Eventueel kan daarbij een aanvraagformulier worden ingevuld.

Beheer: hieronder wordt het inklaarverstaan, dus het fysiek en administratief toevoegen aan de voorraad nadat het reisdocument is ontvangen.

Uitreiking: hieronder wordt verstaan het feitelijk aan de houder ter beschikking stellen van het op zijn naam gestelde waardedocument.

3.4.1 Functiescheiding Reisdocumenten

Op grond van de PUN dient de volgende functiescheiding te worden gerealiseerd:

- Tussen de beveiligingsfunctionaris reisdocumenten en degenen die belast zijn met uitvoerende en beheertaken met betrekking tot reisdocumenten (PUN art. 93, lid 10).
- De beveiligingsfunctionaris reisdocumenten mag niet betrokken zijn bij of verantwoordelijkheid dragen voor de procedures rondom reisdocumenten. Dit voorkomt dat de beveiligingsfunctionaris reisdocumenten zijn eigen werk controleert.
- Tussen aanvraag/verstrekking, beheer en uitreiking van reisdocumenten (PUN art. 93 lid 1, sub c). Het reisdocument moet door een andere medewerker worden uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

De functiescheiding op dit gebied wordt in de gemeente Molenwaard bereikt doordat op het uitreikformulier of het aanvraagformulier de paraaf van de medewerker is geplaatst, die over de aanvraag heeft beslist. De uitreiking vindt plaats door andere medewerker. De meeste uitgaven vinden plaats door AMP Logistics.

- Door de medewerkers wordt er middels de signalering in de reisdocumentenmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt.
- Voorts dient er ingevolge artikel 93, lid 1, sub c van de PUN functiescheiding te zijn gerealiseerd tussen degene die het beheer heeft over de voorraad gepersonaliseerde reisdocumenten en de medewerkers die de aanvraag behandelen dan wel de uitreiking verzorgen.

Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Hierbij gelden op grond van artikel 93, lid 3 van de PUN de volgende voorschriften. Schriftelijk wordt vastgelegd:

- De reden waarom tijdelijk niet aan de eis van functiescheiding kan worden voldaan;
- De periode waarin niet aan de eis van functiescheiding kan worden voldaan;
- De namen van de medewerkers, die in deze periode zijn belast met de aanvraag/verstrekking, het beheer en de uitreiking van de reisdocumenten.

De uitdraai uit het RAAS en de afschriften van de in deze periode verstrekte documenten worden afzonderlijk bewaard. Na afloop van de betreffende periode controleert de beveiligingsfunctionaris reisdocumenten of de schriftelijke vastlegging aanwezig is en de aanvraag/verstrekking, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

Indien hier in de gemeente Molenwaard sprake van zou zijn wordt een procedure Ontbreken van voldoende functiescheiding opgesteld en vastgesteld en conform deze procedure gehandeld.

3.4.2 Functiescheiding Rijbewijzen

Op grond van het Reglement Rijbewijzen dient de volgende functiescheiding te worden gerealiseerd:

- Tussen aanvraag en uitreiking van rijbewijzen
- Het rijbewijs wordt door een andere medewerker uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

De functiescheiding op dit gebied wordt in de gemeente Molenwaard bereikt doordat op het aanvraagformulier de paraaf van de medewerker is geplaatst, die over de aanvraag heeft beslist. Door de medewerkers wordt er middels de signalering in de rijbewijsmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt. De meeste rijbewijzen worden door AMP uitgereikt en na een telefoontje door medewerkers Burgerzaken in de rijbewijsmodule verwerkt.

Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Hierbij gelden op grond van artikel 128, lid 3 van het Reglement Rijbewijzen de volgende voorschriften:

Schriftelijk wordt vastgelegd:

- De reden waarom tijdelijk niet aan de eis van functiescheiding kan worden voldaan;
- De periode waarin niet aan de eis van functiescheiding kan worden voldaan;
- De namen van de ambtenaren, die in deze periode zijn belast met de aanvraag, het beheer en de uitreiking van de rijbewijzen.

De betreffende aanvraagformulieren en de gegevens over de in deze periode verstrekte documenten worden afzonderlijk bewaard.

Na afloop van de betreffende periode controleert de beveiligingsfunctionaris rijbewijzen of de schriftelijke vastlegging aanwezig is en de aanvraag, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

Indien hier in de gemeente Molenwaard sprake van zou zijn wordt een procedure Ontbreken van voldoende functiescheiding opgesteld en vastgesteld en conform deze procedure gehandeld.

OVERZICHT BIJLAGEN

BRP

Verordening Verstrekkingen BRP 2014

Regeling gegevensverstrekking basisregistratie personen Molenwaard

2a. Regeling Bestuurlijke boete

Regeling Beheer en Toezicht BRP

Procedure Autorisatie tot de gemeentelijke voorziening

Procedure Bijhouding van de BRP
Procedure Briefadres
Procedure Correctie
Procedure Identificatie en Machtiging
Procedure Inzagerecht
Procedure Logging van toegang tot en gebruik van de gemeentelijke voorziening (incl communicatie)
Procedure Protocollering
Procedure Reconstructie
Procedure Terugmeldingen
Procedure Verstrekkingbeperking
Procedure Verstrekking van gegevens aan organen van de gemeente
Procedure Verstrekken van gegevens uit de BRP

Bijlage Activiteitenkalender informatiebeveiliging en privacy
17a Bijlage Protocol vermissing personen
18. Bijlage Overeenkomst Cipers Hosting met PinkRoccade
19. Bijlage DAP met PinkRoccade
20. Bijlage SLA met PinkRoccade
21. Bijlage Bewerkersovereenkomst met PinkRoccade
22. Bijlage Brief continuïteit GBA-applicatie in PPC PinkRoccade
23 Procedure PinkRoccade rondom Datalekken
24. Bijlage Draaiboek uitwijktest BRP PinkRoccade
25. Bijlage Draaiboek back-up BRP PinkRoccade

Waardedocumenten

26. Procedure Aanvraag en uitreiking waardedocumenten
27. Procedure Autorisatie RAAS aanvraagstations en rijbewijsmodule
28. Procedure Back-up en restore RAAS
29. Procedure Ontvangst en beheer waardedocumenten

30. Bijlage Activiteitenkalender Waardedocumenten
31. Bijlage Aangewezen medewerkers mobiele vingerapparatuur
32. Bijlage Aangewezen medewerkers waardedocumenten
33. Bijlage Autorisatiebevoegden waardedocumenten
34. Bijlage Formulier Identificatievragen
35. Bijlage Ontvangst- en innamebewijs authenticatiekaart en smartcard
36. Bijlage Ontvangstlijst waardedocumenten
37. Bijlage Convenant BZK-Molenwaard proeftuin bezorgen
38. Bijlage convenant proeftuin bezorgen rijbewijzen
39. Bijlage Dienstverleningsovereenkomst AMP Logistics
39aBijlage dienstverleningsovereenkomst bezorgdienst rijbewijzen
39bBijlage dienstverleningsovereenkomst pre-inklaring rijbewijzen
40. Bijlage Procesbeschrijving bezorging reisdocumenten
41. Bijlage Procedure vermissing en ontvreemding bij bezorging
42. Bijlage Bewerkersovereenkomst AMP Logistics
43. Bijlage Risicoafweging Molenwaard incl. procesbeschrijving (ICTU)

Overig algemeen

44. Procedure Rapportage van specifieke incidenten
45. Procedure Introductie nieuw personeel Burgerzaken
46. Procedure Toegang tot de beveiligde ruimte Burgerzaken
47. Procedure Continuïteit gemeentelijke dienstverlening BRP en Waardedocumenten

48. Bijlage Agressieprotocol gemeente Molenwaard
49. Bijlage Functieverdeling
50. Bijlage Formulier Introductie nieuw personeel Burgerzaken
51. Risico-inventarisatie BRP en Waardedocumenten
52. Protocol vermissing personen

Molenwaard,

Burgemeester en wethouders in haar hoedanigheid als verantwoordelijke voor de BRP.

De burgemeester,

*De heer D.R. van der Borg
De secretaris,
B.J. Nootenboom
Burgemeester in zijn hoedanigheid als verantwoordelijke voor het onderdeel Waardedocumenten.
De burgemeester,
de heer D.R. van der Borg*