GEMEENTE HEERENVEEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Heerenveen

Nr. 20100

27 januari

2020

Beveiligingsrichtlijnen BRP en waardedocumenten 2019

1 Algemeen

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 voor de BRP zijn de burgemeester en de wethouders samen. De Paspoortwet en het Reglement rijbewijzen vallen onder de directe verantwoordelijkheid van de burgemeester.

De verantwoordelijke bestuursorganen moeten jaarlijks rapporteren over de mate waarin en de wijze waarop wettelijke regelgeving wordt gehandhaafd. Aan de getroffen beveiligingsmaatregelen moeten richtlijnen over informatiebeveiliging ten grondslag te liggen. De uitgangspunten en beveiligingsprocedures die invulling aan de gestelde eisen moeten geven zijn in deze richtlijnen opgenomen.

Aan de beveiliging ligt het door het college vastgestelde algemene 'Informatiebeveiligingsplan 2014 gemeente Heerenveen' ten grondslag, waarin de uitgangspunten zijn opgenomen. Deze regeling 'Beveiligingsrichtlijnen BRP en Waardedocumenten' sluit aan op het Informatiebeveiligingsplan 2014 (en opvolgende plannen). De regeling vormt de basis voor de uit te voeren procedures met bijbehorende formulieren en rapportages. Het vormt de invulling van de eisen gesteld in de Wet BRP, de paspoortwet en het Reglement Rijbewijzen.

De bijbehorende procedures, formulieren en rapportages waarnaar wordt verwezen, zijn terug te vinden als opsomming in het hoofdstuk 'Maatregelen'.

1.1 Inleiding

Op basis van de Algemene Verordening Gegevensbescherming (AVG) is de Gemeente Heerenveen verplicht tot het verzorgen van beveiligingsmaatregelen rondom de verwerking van persoonsgegevens. De gemeentelijke processen BRP en waardedocumenten zijn niet de enige processen waarvoor in wetten of reglementen staan voorgeschreven, dat het treffen van beveiligingsmaatregelen noodzakelijk is. De gemeente verwerkt persoonsgegevens ook binnen tal van andere processen, waarbij evengoed wettelijke regels gelden.

Het gemeentebrede informatiebeveiligingsbeleid met daarop afgestemde plannen is nodig om de totale bedrijfsvoering van de gemeente Heerenveen te beveiligen. Deze richtlijnen bevatten specifieke maatregelen, maar zijn voor wat betreft algemene beveiligingsmaatregelen afgestemd op de inhoud van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), opgesteld door de Informatiebeveiligingsdienst voor gemeenten (IBD). Naar verwachting zal dat in 2020 gebeuren op basis van de Baseline Informatiebeveiliging Overheid (BIO).

De Wet Basisregistratie personen (Wet BRP) biedt de nieuwe grondslag voor de basisregistratie van persoonsgegevens 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.

1.2 Totstandkoming, implementatie en evaluatie

1.2.1 Overleggroep Informatiebeveiliging

In 2014 is de Overleggroep Informatiebeveiliging ingesteld. De leden van Overleggroep Informatiebeveiliging richten zich specifiek op de BRP en Waardedocumenten. De leden hebben een sleutelrol in of vergaande kennis van:

- de Wet BRP, de Paspoortwet en het Reglement Rijbewijzen of
- het beheer van de gemeentelijke voorziening of
- het Informatie(beveiligings)beleid of
- het beheer van waardedocumenten of
- de (fysieke) beveiliging van het gemeentehuis.

De Overleggroep Informatiebeveiliging werkt onder verantwoordelijkheid van het hoofd van de afdeling Publiek, in de rol van de beveiligingsbeheerder BRP. De samenstelling is opgenomen in deze regeling als Bijlage A: Functieverdeling BRP en waardedocumenten.

Bij de totstandkoming van de regeling 'Beveiligingsrichtlijnen BRP en waardedocumenten' is deze besproken binnen de Overleggroep Informatiebeveiliging.

1.2.2 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 beveiligingsrichtlijnen zijn deze doelstellingen specifiek gericht op de onderwerpen BRP en waardedocumenten.

Medewerkers moeten (o.a. tijdens werkoverleggen) bij de implementatie en ontwikkeling van het opgestelde beleid worden betrokken en zijn medeverantwoordelijk voor de uitvoering van het beleid. Op basis van hun rollen en taken binnen de organisatie worden verantwoordelijkheden aan hen toegewezen. De Security Officer (CISO) 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.

Het Informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd door de Security Officer (CISO). Deze controleert of de in het beleid opgenomen procedures nog steeds relevant en actueel zijn en stelt deze indien nodig bij. Alle medewerkers van de gemeente Heerenveen worden via de gebruikelijke interne kanalen geïnformeerd over wijzigingen binnen het informatiebeveiligingsbeleid, de regeling 'Beveiligingsrichtlijnen BRP en waardedocumenten' en aanpassingen binnen maatregelen of procedures. Indien nodig kan dit ook via het reguliere werkoverleg plaatsvinden.

Doorgevoerde wijzigingen die direct betrekking hebben op individuele taken en bevoegdheden worden door de leidinggevende, expliciet en rechtstreeks naar de betrokken medewerker gecommuniceerd.

Deze regeling wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de beveiligingsbeheerder BRP en bij noodzaak daartoe bijgesteld.

Deze regeling bevat ook een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden bezien op actualiteit. In deze regeling 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 Overleggroep Informatiebeveiliging het voorliggend regeling 'Beveiligingsrichtlijnen BRP en Waardedocumenten' en de daarbij behorende procedures en bijlagen jaarlijks opnieuw bekijkt op actualiteit en controleert op naleving van de beleidsuitgangspunten.

De beveiligingsbeheerder BRP biedt de aangepaste regeling vervolgens ter advisering aan de directie aan. Daarna wordt het ter vaststelling aangeboden aan de bevoegde bestuursorganen, het college van B&W respectievelijk de burgemeester.

1.3 Inwerkingtreding en citeertitel
Deze regeling treedt in werking met ingang van de dag na de dag van haar bekendmaking.

Gelijktijdig met de inwerkingtreding van deze regeling wordt het plan 'Informatiebeveiliging BRP en Waardedocumenten' (versie 1.0) vastgesteld op 15 december 2015 ingetrokken, evenals eerder vastgestelde plannen 'Informatiebeveiliging GBA en waardedocumenten' (versie 1.0 t/m 4.0).

Deze regeling kan worden aangehaald als: 'Beveiligingsrichtlijnen BRP en waardedocumenten 2019'.

1.4 Goedkeuring
Ter bekrachtiging van de voorliggende regeling 'Beveiligingsrichtlijnen BRP en Waardedocumenten 2019' tekent hieronder de opdrachtgever:

2 Informatiebeveiligingsbeleid

2.1 Informatiebeveiliging
'Informatiebeveiligingsbeleid Gemeente Heerenveen' (vastgesteld in 2019) maakt deel uit van het totale beveiligingsbeleid van de gemeente. Deze is mede gebaseerd op de inhoud van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG).

Het 'Informatiebeveiligingsplan gemeente Heerenveen' omvat het algemene beveiligingsbeleid met betrekking tot de informatievoorziening.

Onder informatiebeveiliging wordt in dit kader verstaan een samenhangend geheel van maatregelen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens garandeert en de controleerbaarheid van de getroffen maatregelen.

2.2 Raakvlakken met ander beleid
De regeling 'Beveiligingsrichtlijnen BRP en Waardedocumenten' sluit aan op het 'Informatiebeveiligingsplan gemeente Heerenveen' en richt zich daarbij specifiek op de BRP en de waardedocumenten (hier: reisdocumenten en rijbewijzen).

Het 'Informatiebeveiligingplan gemeente Heerenveen' heeft raakvlakken met het beleid en de daaruit voortvloeiende procedures die zijn gericht op de operationele veiligheid van het uitgifte- en beheerproces van waardedocumenten.

Binnen dit beleidsterrein kan onderscheid gemaakt worden tussen fysieke, logische en organisatorische beveiligingsmaatregelen, met als te noemen voorbeelden: identificatie van gebruikers, sleutelbeleid, personeelsbeleid en het 'clean desk'-beleid.

2.3 Beleidsdoelstelling
Het gemeentebestuur van Heerenveen 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 Heerenveen 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.

Als concrete norm voor de realisering van de beleidsdoelstellingen wordt de eis neergelegd dat de informatiesystemen zoals aangeduid in deze regeling, tijdens reguliere kantoortijden voldoen aan de beschikbaarheidseis van 99%.

Buiten aangegeven tijden, zie paragraaf 2.6.1.1., worden er geen eisen gesteld aan de beschikbaarheid van de systemen met uitzondering van voorzieningen die in het kader van rampenbestrijding zijn getroffen.

2.4 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 moeten nemen. Zo moeten organisaties moderne techniek gebruiken om persoonsgegevens te beveiligen. Verder moeten ze niet alleen naar de techniek kijken, maar ook naar hoe ze als organisatie met persoonsgegevens omgaan.

De Autoriteit Persoonsgegevens (AP) kan de verantwoordelijke voor de verwerking van persoonsgegevens, bij gemeenten doorgaans het college van B en 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 AVG dient het gemeentebestuur ook rekening te houden met de beveiligingseisen die andere wetten stellen, zoals dat voor deze richtlijnen zijn: de Wet BRP, de Paspoortwet en het Reglement rijbewijzen. De beveiliging van de BRP is geregeld bij en krachtens de Wet BRP.

2.5 Taken, verantwoordelijkheden en bevoegdheden
De bestuurlijke verantwoordelijkheid voor de richtlijnen beveiliging BRP en waardedocumenten ligt bij het college van B en W respectievelijk de burgemeester. Deze organen laten de richtlijnen opstellen en zien toe op de uitvoering daarvan.

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

De Informatiebeheerder BRP is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van de richtlijnen voor de gemeentelijke voorzieningen waarmee de gemeente Heerenveen uitvoering geeft aan de Wet BRP en waardedocumenten.

De controller Informatiebeveiliging BRP is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van de richtlijnen Informatiebeveiliging 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).

2.5.1 Verantwoordelijkheden gemeentebestuur
Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Heerenveen. Het college van B&W stelt in deze regeling de beveiligingsrichtlijnen BRP vast en de burgemeester stelt het onderdeel Waardedocumenten vast.

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

Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van de richtlijnen BRP en waardedocumenten is de rol van de *informatiebeheerder BRP* in het leven geroepen. Deze heeft de verantwoordelijkheid om namens de bestuursorganen toe te zien op naleving van de specifieke beveiligingsmaatregelen en -procedures zoals uitgewerkt in de regeling 'Beveiligingsrichtlijnen BRP en waardedocumenten' en daarover aan het college van B en W respectievelijk de burgemeester te rapporteren.

2.5.2 Verantwoordelijkheden van de directie
Beveiliging is op ambtelijk niveau de verantwoordelijkheid van de directie van de gemeente Heerenveen.

De directie 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:
- De voortgang realisatie beveiligingsmaatregelen als beschreven in de regeling 'Beveiligingsrichtlijnen BRP en Waardedocumenten' en gerapporteerd door de beveiligingsbeheerder BRP;
- Het benoemen van mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen;
- De 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;
- Het geven van zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen;
- Het bevorderen van het beveiligingsbewustzijn;
- De herziening en goedkeuring beveiligingsbeleid en de toegekende verantwoordelijkheden.

2.5.3 Verantwoordelijkheden Chief Information Security Officer (CISO)
De Chief Information Security Officer (CISO) is op gemeentelijk niveau verantwoordelijk voor de informatiebeveiliging. 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 moeten kunnen beoordeeld.

De CISO is verantwoordelijk voor:
- het opstellen van het algemene Informatiebeveiligingbeleid;
- de voortgang en de realisatie van beveiligingsmaatregelen zoals beschreven in de richtlijnen;
- het actualiseren van het algemene Informatiebeveiligingsplan;
- het gezamenlijk met informatiebeheerder afstemmen van de maatregelen op afdelingsniveau.

Tevens dient de CISO:
- rechtstreeks te rapporteren aan de gemeentesecretaris;
- gevraagd en ongevraagd de informatiebeveiliging van de gemeente Heerenveen te bevorderen;
- de rapportages over de status te verzorgen en te bekijken of de getroffen maatregelen worden nageleefd en tevens de uitkomsten te evalueren, evenals het doen van voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente Heerenveen.

2.5.4 Verantwoordelijkheden van overige rollen / functies
De verantwoordelijkheden van de rollen en/of functies van de gegevensbeheerder BRP, privacybeheerder BRP, applicatiebeheerder BRP, systeembeheerder BRP en beveiligingsbeheerder BRP zijn vastgelegd in de Regeling Beheer en Toezicht BRP.

Voor alle in de 'Beveiligingsrichtlijnen BRP en waardedocumenten' voorkomende functies is ook de vervanging vastgelegd (zie: Bijlage A: Functieverdeling BRP en waardedocumenten).

2.6 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 Heerenveen.

Een passend beveiligingsniveau
Een adequaat niveau van beveiliging van persoonsgegevens kan worden bereikt door het treffen 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,
- De stand van de techniek,
- De kosten van de treffen maatregelen.

2.6.1 Kwaliteitsaspecten
Informatiebeveiligingsbeleid omvat een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijke top duidelijk maken aan het tactisch en operationeel niveau welke gedragslijn de gemeente Heerenveen dient te volgen om te komen tot een adequate informatiebeveiliging. Het beleid vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Naast het maken en vaststellen van beveiligingsbeleid is het nodig dat de uitgangspunten in een informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient de directie 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:

1e:	**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.
2e:	**integriteit**	De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
3e:	**vertrouwelijkheid**	Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.
4e:	**controleerbaarheid**	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 Heerenveen hanteert voor deze kwaliteitsaspecten de volgende normen:

2.6.1.1 Norm voor beschikbaarheid
Het college van B&W en de directie zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening wordt gestaakt met gevolg dat een aantal bedrijfskritische applicaties niet meer kunnen 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. Deze zijn op werkdagen:
- van 8.30-13.00 uur en van 14.00-16.00 uur en
- donderdagavond van 18.00-20.00 uur.

De (informatievoorziening met betrekking tot de) BRP moet tijdens de openingstijden van het gemeentehuis nagenoeg permanent beschikbaar zijn. In cijfers uitgedrukt betekent dit op jaarbasis een beschikbaarheid van 99,0% Dat is (34½ uur * 50 wk * 1% =) maximaal 17 uren uitval op jaarbasis.

Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt op jaarbasis op werkdagen tijdens kantooruren voor 98,5% beschikbaar te zijn.

Met kantooruren worden hier bedoeld: Maandag, dinsdag en woensdag van 07.15 – 18.30 uur; donderdag van 07.15 – 20.30 uur en vrijdag van 07.15 – 17.00 uur. Dat betekent een norm van maximaal per jaar (56½ uur * 50 weken * 1,5% =) 42 uur niet beschikbaar/uitval in totaliteit. De mogelijkheid om zelfs buitengenoemde kantoortijden, (thuis) te werken, wordt niet meegenomen in de normering van beschikbaarheid.

De momenten van uitval worden via TOPdesk geregistreerd of 'handmatig' bijgehouden door de coördinator van team Burgerzaken. Bij afname van de beschikbaarheid, tot een zorgelijk niveau, wordt dat besproken met het afdelingshoofd Publiek. Deze gaat in overleg met afdelingshoofd Informatiemanagement & ICT waarbij de uitval, de gevolgen en de acties worden besproken om de beschikbaarheid te borgen. Ook het afdelingshoofd I&I kan, op basis van signalen, het initiatief nemen voor een dergelijk overleg.

Aangezien de BRP in beheer is bij de landelijke overheid, is de gemeente voor de realisatie van deze norm afhankelijk van de landelijke beheerder. Voor de continuïteit van de eigen bedrijfsvoering is het noodzakelijk dat de gemeente voorzieningen treft, die onverhoopte storingen binnen het landelijke systeem kunnen opvangen.

Voor de continuïteit in de eigen bedrijfsvoering treft de gemeente ook voorzieningen die onverhoopte uitval van het eigen systeem kan opvangen. Dit betreft voorzieningen die betrekking hebben op de gegevensbestanden, netwerkverbindingen en deze lokale systemen.

Een uitval mag nooit langer duren dan 48 uur. Er zijn adequate voorzieningen getroffen (opgenomen in het Calamiteitenplan) om te borgen dat, ook in geval van calamiteiten, na maximaal 48 uur de dienstverlening aan de burger én aan andere bestuursorganen hervat is.

2.6.1.2 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 het is niet realistisch om dit als concrete eis te stellen. Ten behoeve van het evaluatie instrument zijn kwaliteitsindicatoren opgesteld omtrent 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 is het onderscheid in zes klassen van belang:

Klasse	Omschrijving	Wettelijke norm
A	Persoon en Overlijden	99,7%
B	Adres	99,7%
C	Relaties	99,6%
D	Identificatienummers en nationaliteit	99,5%
E	Overige algemeen	99,5%
F	Administratief	99,4%

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

2.6.1.3 Norm voor vertrouwelijkheid
Uitsluitend bevoegde personen ~in dienst van of werkzaam ten behoeve van de gemeente Heerenveen~ hebben toegang tot voor hen relevante registraties. Daarbinnen kunnen zij gebruik maken van 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. Personen die belast zijn met de bijhouding van BRP gegevens en/of werken met waardedocumenten dienen een geheimhoudingsverklaring te hebben ondertekend.

2.6.1.4 Norm voor controleerbaarheid

Mutaties in persoonsgegevens in de BRP kunnen gevolgen hebben. 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 ook gecontroleerd moet kunnen worden wie welke mutatie heeft verwerkt. De gemeente Heerenveen kent als norm dat 100% van alle mutaties in persoonsgegevens herleidbaar moeten zijn tot de individuele persoon die voor de mutatieverwerking verantwoordelijk was en dat geldt ook voor alle raadplegingen op het niveau van de ingezetene zelf.

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 deze regeling 'Beveiligingsrichtlijnen BRP en Waardedocumenten' opgenomen procedures hebben als doel te voorkomen dat de risico's, behorend bij de aan de verwerking van persoonsgegevens verbonden risicoklasse (II), zich voordoen. Uitvoering van de procedures maakt het bedrijfsproces controleerbaar uit oogpunt van beveiliging.

3 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 nodig 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 wet voorschrijft. Als grondslag voor het beveiligingsbeleid op het onderdeel BRP in deze regeling 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. Bovendien geldt op grond van artikel 4.3 wet BRP de verplichting om jaarlijkse uiterlijk op 31 december 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

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.

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, bijschrijvingsstickers, 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 deze regeling 'Beveiligingsrichtlijnen 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 rijbewijzen en de functiescheiding.

3.2 Periodieke zelfevaluatie, onderzoek en accountantscontrole

3.2.1 Zelfevaluatie

De in deze richtlijnen BRP en waardedocumenten voorgestelde beveiligingsmaatregelen en -procedures vormen voor 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 door de burgemeester aangaande reisdocumenten, naar de Rijksdienst voor Identiteitsgegevens gezonden en openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. De Kwaliteitsmonitor is 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 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 beveiligingsbeheerder 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.

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

3.2.4 Onderzoek Paspoorten en NIK

Sinds april 2013 gebruiken gemeenten voor haar onderzoek naar het reisdocumentenproces de vragenlijst uit de Kwaliteitsmonitor van de Rijksdienst Identiteitsgegevens. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks 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 Beveiligingsfunctionaris reisdocumenten en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan het college van B en W. De burgemeester, ondertekent de rapportage en stuurt deze vóór 14 februari naar de Rijksdienst voor Identiteitsgegevens.

De Beveiligingsfunctionaris waardedocumenten 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 worden 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 de informatiebeheerder, de gegevensbeheerder, de privacybeheerder, de applicatiebeheerder en de systeembeheerder. De beheerrollen ondergaan verandering, zodra de gemeente aansluit op de BRP-voorzieningen en de GBA-voorzieningen afsluit.

Op het gebied van de waardedocumenten dient te worden aangewezen een Beveiligingsfunctionaris reisdocumenten, de Autorisatiebevoegde reisdocumentenstation, de Autorisatiebevoegde aanvraagstation, de Beveiligingsfunctionaris rijbewijzen en de Autorisatiebevoegde rijbewijzen.

De beschrijving en toekenning van de rollen in het kader van de waardedocumenten maken deel uit van deze regeling. (zie: Bijlage B: Functies waardedocumenten.)

Voor alle in dit hoofdstuk voorkomende functies is de vervanging vastgelegd. (zie: Bijlage A: Functieverdeling BRP en waardedocumenten.)

3.4 Functiescheiding Waardedocumenten
Om de kans te verkleinen dat medewerkers van de afdeling Publiek 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: 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: de verantwoordelijkheid voor de materialen en (gepersonaliseerde) waardedocumenten tussen het moment van de aanvraag en de uitreiking.
- Uitreiking: 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.

- Functiescheiding wordt afgedwongen door de applicatie waarin de reisdocumenten worden aangevraagd en uitgereikt.
- 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 Reisdocumenten Aanvraag en Afgifte Station (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.

3.4.2 Functiescheiding Rijbewijzen
Op grond van het Reglement Rijbewijzen dient tussen aanvraag en uitreiking van rijbewijzen te worden gerealiseerd. Het rijbewijs wordt door een andere medewerker uitgereikt dan degene die de beslissing op de aanvraag heeft genomen. Deze functiescheiding wordt afgedwongen in de applicatie waarin de rijbewijzen worden aangevraagd en uitgereikt.

Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Op grond van artikel 128, lid 3 van het Reglement Rijbewijzen wordt dan schriftelijk 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 verstrekte documenten worden, in deze periode van onvoldoende functiescheiding, 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.

4 Maatregelen
Jaarlijks extern toezicht via ENSIA, Eenduidige Normatiek Single Information Audit) helpt gemeenten in één keer slim verantwoording af te leggen over algemeen informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG). 2019 is het laatste jaar dat er verantwoording over de BIG wordt afgelegd. In 2020 zal dat gebeuren op basis van de Baseline Informatiebeveiliging Overheid (BIO).
Het ENSIA stelsel is in beheer bij VNG Realisatie en is een initiatief van:
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (DGBRW)
- Ministerie van Sociale Zaken en Werkgelegenheid
- Vereniging van Nederlandse Gemeenten.

De verantwoordingssystematiek, de integrale horizontale verantwoording, is samengevoegd en gestroomlijnd over:
- Basisregistratie Personen (BRP),
- wet- en regelgeving Reisdocumenten (PUN en PNIK),
- Digitale persoonsidentificatie (DigiD),
- Basisregistratie Adressen en Gebouwen (BAG),
- Basisregistratie Grootschalige Topografie (BGT),
- Basisregistratie Ondergrond (BRO) en
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

Naast de algemene beveiligingsmaatregelen, die binnen ENSIA zijn opgenomen, is het voor elk genoemd onderdeel van belang om te voldoen aan ‘eigen’ specifieke beveiligingsnormen. Via onder andere de Zelfevaluatie BRP en de Zelfevaluatie PNIK wordt jaarlijks (de verticale) verantwoording afgelegd.

Daarbij vult het ENSIA stelsel op onderdelen aan. Een uittreksel van de resultaten wordt gezonden aan de Rijksdienst voor Identiteitsgegevens (RVIG) en de Autoriteit Persoonsgegevens.

Voor de BRP en waardedocumenten, zoals gesteld in het juridisch kader (zie 1.2) en de beleidsdoelstellingen (zie 2.3) van deze regeling, zijn er daarom ook specifieke maatregelen nodig.

4.1 Procedures
Een van de maatregelen is het vastleggen van processen in vaste werkwijzen. Deze werkwijzen zijn vastgelegd in procedures. (zie Bijlage C: Opsomming vastgelegde procedures). Deze procedures hebben als doel:
- het borgen van een eenduidige werkwijze;
- het verhogen van de efficiency;
- bevoegdheden, verantwoordelijkheden en taken inzichtelijk maken;
- het voldoen aan wettelijke normen.

Per kalenderjaar worden in ieder geval twee procedures grondig geanalyseerd, de overige procedures worden op hoofdlijnen nagelopen. Zo nodig worden actualisaties doorgevoerd.

De vastgelegde procedures zijn opgenomen in een software programma; thans: IC Content. Medewerkers van de afdeling Publiek zijn of worden geautoriseerd de procedures te raadplegen die gerelateerd zijn aan hun functie, taak en rol.

4.2 Overige maatregelen
Om na te gaan of de procedures juist worden gevolgd en om eventuele tekortkomingen te constateren, worden de procedures, vermeld in dit hoofdstuk en in bijlage C, periodiek gecontroleerd door de Controller Informatiebeveiliging BRP.

Naast deze uit te voeren controles zijn er ook overige maatregelen genomen:
- Gebruik van de Kwaliteitsmonitor; een maatregel/hulpmiddel vanuit de Rijksdienst voor identiteitsgegevens (de RvIG) om te controleren hoe gemeente Heerenveen er voor staat voor wat betreft de kwaliteit van gegevens én de processen rond de BRP en het reisdocumentenproces;
- Deelname aan de Landelijke Aanpak Adreskwaliteit (LAA), waardoor de kwaliteit van de BRP verhoogd wordt.

4.3 Doorontwikkeling
Het is van belang om beveiligingsrichtlijnen voortdurend te verbeteren. Dit gebeurt bijvoorbeeld naar aanleiding van actiepunten of aanbevelingen uit de jaarlijkse rapportages van de Zelfevaluatie BRP en de Zelfevaluatie Waardedocumenten.

4.4 Beleid actualiseren
Bij het opstellen van de regeling 'Beveiligingsrichtlijnen BRP en waardedocumenten 2019' zijn de volgende verordeningen en regelingen geraadpleegd, inhoudelijk getoetst en zijn of worden zo nodig actualisaties voorgedragen:

beschrijving	***vastgesteld***
Verordening gegevensverstrekkingen BRP	30-06-2014
Reglement gegevensverstrekkingen BRP en bijlagen (tabellen)	Dec 2019
Regeling Beheer en toezicht BRP met bijlagen	Dec 2019
Regeling briefadres en Toelichting op de Regeling briefadres	Dec 2019
Beleidsregel bestuurlijke boete Basisregistratie personen	16-09-2014

Heerenveen, 10 december 2019.

Burgemeester en wethouders in haar hoedanigheid als verantwoordelijke voor de BRP.
De burgemeester,
De heer T.J. van der Zwan

De secretaris,
de heer J. van Leeuwestijn

Burgemeester in zijn hoedanigheid als verantwoordelijke voor het onderdeel Waardedocumenten.
De burgemeester,
de heer T.J. van der Zwan

Bijlage A: Functieverdeling BRP en waardedocumenten

Binnen de gemeente Heerenveen zijn, in het kader van de Regeling Beveiligingsrichtlijnen BRP en waardedocumenten, de volgende personen aangewezen:

Leden Overleggroep Informatiebeveiliging:
- Arjen Glas
- Erik Brands
- Gerben Aukema
- Henk ten Boom
- Klaas Hoekstra
- Martin de Jong
- Auke de Haan, Irma Brouwer en Janna Ellen
- Evert Kleiterp

Leden uitwijkteam BRP en waardedocumenten:
- Rixt Veurman
- Judica Kluit
- Frans Douwenga
- Silvester Wijnia
- Jeroen van der Laan
- Evert Kleiterp
- Auke de Haan

Wie is wie:

Functie	*In persoon*	*plaatsvervangend*
De gemeentesecretaris	Jeroen van Leeuwestijn	Marion Mulder
Hoofd afdeling Publiek	Arjen Glas	Ria Soet
Interne uitwijkcoördinator BRP	Rixt Veurman	Jaap Tanis
Informatiebeheerder BRP	Arjen Glas	Ria Soet
Systeembeheerder BRP	Evert Kleiterp	Frans Douwenga
Applicatiebeheerder BRP	Auke de Haan	Irma Brouwer Janna Ellen
Beveiligingsbeheerder BRP	Martin de Jong	Klaas Hoekstra
Fraudecoördinator BRP	Klaas Hoekstra	Martin de Jong
Gegevensbeheerder BRP	Klaas Hoekstra	Martin de Jong
Privacybeheerder BRP	Klaas Hoekstra	Martin de Jong
Controller Informatiebeveiliging BRP	Gerben Aukema	Henk ten Boom
Chief Information Security Officer (CISO)	Erik Brands	Henk Post neemt contact op met de poule van CISO's (gemeente Súdwest-Fryslân, Waadhoeke, Harlingen, De Fryske Marren, Smallingerland)
Beveiligingsfunctionaris reisdocumenten én waardedocumenten	Gerben Aukema	Henk ten Boom
Autorisatiebevoegde Reisdocumentenstation	Klaas Hoekstra	Klaas Luinenburg
Autorisatiebevoegde aanvraagstation	Annette Tjoelker, Henriëtte Poortinga, Ilja Kroon, Niels Peek, René ter Schuur, Zaina Oukoums, Klaas Hoekstra	
Autorisatiebevoegde rijbewijzen	Klaas Hoekstra	Klaas Luinenburg

Bijlage B: Functies waardedocumenten

Beveiligingsfunctionaris reisdocumenten (afgekort BR)

Plaats in de organisatie
Op grond van artikel 93 van de PIJN 2001 moet door de burgemeester een BR zijn aangewezen. De BR is rechtstreeks verantwoording schuldig aan de burgemeester zonder tussenkomst van de leidinggevenden in de lijn.

De BR is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures reisdocumenten. De taken en verantwoordelijkheden van deze functionaris dienen in een functiebeschrijving te zijn opgenomen.

De BR dient in staat gesteld te worden zijn taken onafhankelijk van de uitvoering van taken en werkprocessen met betrekking tot het aanvragen, beheer en de uitgifte van reisdocumenten uit te voeren.

Van de aanwijzing of de vervanging van de BR moet schriftelijk melding worden gedaan aan de Rijksdienst voor Identiteitsgegevens (de RvIG).

Functiebeschrijving

Taken en verantwoordelijkheden
De BR is verantwoordelijk voor:
- De controle (steekproefsgewijs) op de naleving van de beveiligingsprocessen, -procedures en instructies betreffende reisdocumenten mede aan de hand van de normeringen uit de Zelfevaluatie Reisdocumenten;
- De controle op een juiste afhandeling van de Zelfevaluatie Reisdocumenten;
- Het (laten) verrichten van onderzoek bij beveiligingsincidenten met het doel dergelijke situaties in de toekomst te voorkomen;
- Het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten/tekortkomingen in de beveiligingsvoorzieningen.

Daarnaast kent de BR de volgende algemene beveiligingstaken met betrekking tot reisdocumenten, waarvoor hij tevens verantwoordelijk is:
- het bewaken van uit te voeren acties voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van de 'Regeling Beveiligingsrichtlijnen BRP en waardedocumenten';
- het toezicht houden op de actualiteit van de'Regeling Beveiligingsrichtlijnen BRP en waardedocumenten', de beveiligingsprocessen, -procedures/afspraken en instructies;
- gevraagd en ongevraagd advies geven aan de burgemeester en de directie over verbeteringen ten aanzien van de beveiliging;
- het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures;
- het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en -processen;
- het toezicht houden of (nieuwe) medewerkers worden geïnstrueerd en bekendgemaakt met de beveiligingsprocedures en -processen met betrekking tot reisdocumenten;
- het registreren van de meldingen van beveiligingsincidenten;
- het rapporteren aan de burgemeester betreffende de stand van zaken van beveiliging, eventueel naar aanleiding van bijzonderheden/incidenten;
- Het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

Autorisatiebevoegde reisdocumentenstation/-aanvraagstation

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties stelt per uitgiftelocatie identificatiekaarten, opstartkaarten en een authenticatiekaart ter beschikking waarmee toegang wordt verleend tot het Reisdocumenten Aanvraag en Archiefstation (RAAS), de aanvraagstations en het Mobiel vingerafdrukopname-apparaat (MVA).

Identificatiekaarten
Met een identificatiekaart krijgt een persoon op elektronische wijze toegang tot het RAAS en de daarin opgeslagen programmatuur en gegevens. Per uitgiftelocatie worden ten minste twee en ten hoogste 20 identificatiekaarten beschikbaar gesteld.

Authenticatiekaart MVA
Met een authenticatiekaart krijgt een persoon toegang tot het MVA om vingerafdrukken plaatsonafhankelijk op te nemen. Per MVA wordt één authenticatiekaart beschikbaar gesteld. De ABR wijst maximaal drie personen aan die aanvragen met het MVA in behandeling mogen nemen.

Opstartkaart
Met de opstartkaarten kunnen de aanvraagstations in werking worden gesteld. Per aanvraagstationlocatie worden twee opstartkaarten beschikbaar gesteld.

De kaarten worden opgeslagen volgens artikel 91 van de Paspoortuitvoeringsregeling Nederland 2001(PUN).
De opslagvoorziening voldoet minimaal aan de volgende eisen:
- *Een brandwerende en inbraakvertragende voorziening (kluiskast) die genormeerd is op basis van € 1.000 waardebergingsindicatie.*
- *De voorziening is in een afsluitbare ruimte geplaatst.*
- *De afgesloten ruimte is voorzien van een inbraakdetectiesysteem die in verbinding staat met een door de rijksoverheid toegelaten alarmcentrale.*
- *De ruimte is niet toegankelijk voor onbevoegden.*

De Autorisatiebevoegden reisdocumentenstation (ABR) en Autorisatiebevoegden aanvraagstation (ABA) zijn verantwoordelijk voor de autorisaties, het gebruik, de bewaring en het bijhouden van een registratie van de kaarten. Vaak worden beide functies door dezelfde personen uitgevoerd.

Voor het gebruik van de identificatiekaarten en authenticatiekaart zijn de ABR en ABA verantwoordelijk voor het bijhouden van een volledige registratie. Het is belangrijk om het gebruik en de bewaring te registreren, omdat uit deze registratie kan worden vastgesteld welke personen op bepaalde data toegang hadden tot het systeem en de gegevens. De registratie moet minimaal de volgende gegevens bevatten:
- alle beschikbare kaarten;
- waar en hoe deze worden bewaard (binnen en buiten werktijd);
- wie op welk moment een kaart in gebruik heeft;
- wanneer en van wie kaarten zijn of worden ingetrokken en
- wanneer kaarten zijn vernietigd.

Deze beheersactiviteiten worden periodiek gecontroleerd en er wordt een verslag van deze controle opgemaakt.

De leverancier houdt een registratie bij van de uitgegeven en vermiste opstartkaarten. Bovendien is het praktisch als de ABR ook een registratie bijhoudt van de opstartkaarten die in bezit zijn. Zeker bij verlies is het handig als het kaartnummer bekend is voor het opmaken van een proces-verbaal bij de politie.

De ABR
De burgemeester wijst per uitgiftelocatie tenminste twee medewerkers aan als ABR die binnen het aanvraagsysteem reisdocumenten kunnen functioneren overeenkomstig de gebruikershandleiding bij het aanvraagstation bedoeld in artikel 87 van de PIJN.

De ABR legt, rechtstreeks of indirect, verantwoording af aan de burgemeester.

Het hoofd van de afdeling Publiek vult omtrent de aanwijzing of vervanging van een ABR het daarvoor bedoelde formulier in en zendt deze aan IDEMIA.

De ABR is verantwoordelijk voor:
- het autorisatiebeheer van de identificatiekaarten;
- de bewaring van de identificatiekaarten;
- de registratie van personen aan wie in een bepaald tijdvak een kaart verstrekt is.
  Het RAAS registreert slechts een deel van de gegevens die voor de verantwoordelijke van belang zijn: zo wordt bijvoorbeeld niet geregistreerd aan wie in een bepaald tijdvak een kaart verstrekt is. De ABR is eindverantwoordelijke voor het bijhouden van een volledige registratie.

De ABR neemt de identificatiekaarten en de bijbehorende codes in ontvangst.
Vervolgens worden de identificatiekaarten door de ABR in het RAAS ingeklaard.
Direct na het inklaren heeft de ABR de volgende keuzes:
- *De kaart direct koppelen aan een gebruiker*
  De gebruiker wijzigt direct na ingebruikname van de identificatiekaart de pincode. De pincode wordt periodiek door de gebruiker gewijzigd.
- *De kaart niet direct koppelen aan een gebruiker*
  De ABR bewaart de pinmailer en de identificatiekaart afzonderlijk van elkaar of de pincode wordt direct in een eigen bewaarcode gewijzigd die alleen bij de ABR bekend is.

Gekoppelde identificatiekaarten worden uitsluitend gebruikt door de gebruiker die aan de kaart is gekoppeld. Het uitlenen van de kaart en code aan collega's is verboden. Indien kaarten niet worden gebruikt, zijn deze op de voorgeschreven wijze opgeslagen.
Voor meer informatie over het koppelen, intrekken e.d. van identificatiekaarten wordt de gebruikershandleiding RAAS.
De geautoriseerde medewerker van het team Burgerzaken, die toegang heeft tot het Reisdocumenten Aanvraag en Archiefstation (RAAS):

- *ontvangt hiervoor een persoonsgebonden identificatiekaart in combinatie met een persoonlijke pincode;*
- *tekent voor ontvangst van de persoonsgebonden identificatiekaart en bijbehorende pincode;*
- *wijzigt deze pincode direct na ontvangst;*
- *wijzigt de pincode minimaal 1x per jaar.*

De persoonsgebonden identificatiekaarten en pincodes worden:

- *nooit uitgeleend of bekend gemaakt aan anderen;*
- *altijd gescheiden bewaard van de pincodes en opgeborgen in een beveiligde ruimte.*

De ABR ziet toe op naleving hiervan.
De ABR is verantwoordelijk voor het autorisatiebeheer, de bewaring van de identificatiekaarten (max 20 stuks) en de registratie van de personen aan wie hij in een bepaald tijdvak een kaart verstrekt.

De ABR draagt zorg voor terugzending van de persoonsgebonden identificatiekaarten, indien deze niet meer worden gebruikt. Deze worden, vergezeld van de hiertoe bestemde formulieren, teruggestuurd aan de producent.

De ABR registreert in het reisdocumentenstation de intrekking van identificatiekaarten indien deze na verlies, diefstal of defect verloren zijn gegaan of onbruikbaar zijn geworden of anderszins niet langer gebruikt mogen worden.

De ABR draagt zorg voor de vernietiging van ingetrokken identificatiekaarten voor zover deze in zijn bezit zijn en geen nader onderzoek daaraan hoeft plaats te vinden.

De leverancier IDEMIA houdt een registratie bij van de uitgegeven en ingetrokken identificatiekaarten.

De ABA
De burgemeester wijst per aanvraagstation tenminste twee medewerkers aan, die zullen functioneren als ABA overeenkomstig de gebruikershandleiding bij het aanvraagstation bedoeld in artikel 87 van de PIJN.

De burgemeester kan deze taken mandateren aan het hoofd van de afdeling Publiek.
De ABA is verantwoordelijk voor:

- de bewaring van de authenticatiekaart MVA en de opstartkaarten;
- het gebruik van de authenticatiekaart MVA en de opstartkaarten.

De ABA neemt de authenticatiekaart MVA en de opstartkaarten in ontvangst.
Deze zijn niet persoonsgebonden en wordt niet ingeklaard in het RAAS.
Voor het gebruik van het aanvraagstation wordt de medewerker een gebruikersnaam toegekend en wordt diens vingerafdruk(ken) opgenomen.

De authenticatiekaart wordt uitsluitend gebruikt door de daartoe aangewezen gebruikers. De burgemeester of de daartoe aangewezen ambtenaar benoemt maximaal drie personen die vingerafdrukken met behulp van het MVA mogen opnemen. Als de kaart niet gebruikt wordt, is deze op de voorgeschreven wijze opgeslagen.

De opstartkaart gebruikt de medewerker door deze te plaatsen in de kaartlezer van het aanvraagstation.

Om verlies en per abuis vernietiging te voorkomen wordt, direct na het opstarten van het aanvraagstation, de opstartkaart weer opgeborgen op een vaste plek.
Bij verlies of vernietiging van een opstartkaart moeten alle aanvraagstations vervangen worden, tenzij bij vernietiging zichtbaar kan worden aangetoond dat de opstartkaart per abuis door een medewerker vernietigd (versnipperd) is.

Beveiligingsfunctionaris rijbewijzen
Op grond van artikel 128, lid 6 van het Reglement Rijbewijzen moet door de burgemeester een Beveiligingsfunctionaris rijbewijzen zijn aangewezen.

Deze Beveiligingsfunctionaris rijbewijzen is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures rijbewijzen. De taken en verantwoordelijkheden van deze functionaris dienen in een functiebeschrijving te zijn opgenomen.

De Beveiligingsfunctionaris rijbewijzen is rechtstreeks verantwoording schuldig aan de burgemeester. De Beveiligingsfunctionaris rijbewijzen is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van rijbewijzen en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

Functiebeschrijving

Plaats in de organisatie
De Beveiligingsfunctionaris rijbewijzen wordt op grond van artikel 128 van het Reglement Rijbewijzen benoemde door de burgemeester. Daarbij dient in ieder geval sprake te zijn van functiescheiding tussen deze beveiligingsfunctie en de uitvoerende taken met betrekking tot de afgifte en het beheer van rijbewijzen. De Beveiligingsfunctionaris rijbewijzen is rechtstreeks verantwoording schuldig aan de burgemeester zonder tussenkomst van de leidinggevenden in de lijn.

Taken en verantwoordelijkheden
De Beveiligingsfunctionaris rijbewijzen is verantwoordelijk voor:
- de controle (steekproefsgewijs) op de naleving van de beveiligingsprocessen, -procedures en instructies betreffende rijbewijzen;
- het (laten) verrichten van onderzoek bij beveiligingsincidenten, met het doel dergelijke situaties in de toekomst te voorkomen;
- het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten/tekortkomingen in de beveiligingsvoorzieningen.

Daarnaast kent de Beveiligingsfunctionaris rijbewijzen de volgende algemene beveiligingstaken met betrekking tot rijbewijzen, waarvoor hij tevens verantwoordelijk is:
- het bewaken van uit te voeren acties ter verbetering voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van het plan Informatiebeveiliging BRP en Waardedocumenten;
- het toezicht houden op de actualiteit van de 'Regeling Beveiligingsrichtlijnen BRP en Waardedocumenten', de beveiligingsprocessen, -procedures/afspraken en instructies;
- gevraagd en ongevraagd advies geven aan de burgemeester en de directie over verbeteringen ten aanzien van beveiliging;
- het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures;
- het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en -processen;
- het toezicht houden of (nieuwe) medewerkers worden geïnstrueerd en bekendgemaakt met de beveiligingsprocedures en -processen met betrekking tot de rijbewijzen;
- het registreren van de meldingen van beveiligingsincidenten;
- het rapporteren aan de burgemeester betreffende de stand van zaken van beveiliging, eventueel naar aanleiding van bijzonderheden/incidenten;
- het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

Autorisatiebevoegde rijbewijzen
De burgemeester wijst per uitgiftelocatie tenminste twee medewerkers aan als Autorisatiebevoegde rijbewijzen. De Autorisatiebevoegde rijbewijzen legt rechtstreeks verantwoording af aan de burgemeester.

Het hoofd van de afdeling Publiek vult omtrent de aanwijzing of vervanging van een Autorisatiebevoegde rijbewijzen het daarvoor bedoelde formulier in en zendt deze aan de RDW.

Een smartcard is een pasje met daarop een chip. De smartcard wordt gebruikt om in te loggen in het Backoffice station. Op de chip zijn de gegevens van de certificaathouder opgeslagen. Er is een Autorisatie Bevoegde persoon voor Rijbewijzen (ABR) smartcard en een Rijbewijs Afgifte (RYA) smartcard.

De Autorisatiebevoegde rijbewijzen is de medewerker die bevoegd is om de autorisaties voor rijbewijzen te beheren, dat wil zeggen dat hij/zij:
- autorisaties toekent, beheert en beëindigt;
- autorisaties en eventuele wijzigingen daarin aanmeldt bij de RDW;
- registreert aan wie deze autorisaties zijn verstrekt;
- toezicht houdt op het zorgvuldig gebruik van deze autorisaties.

De medewerker met een ABR-smartcard is bevoegd om:

- andere medewerkers (inclusief een andere Autorisatiebevoegde rijbewijzen) te autoriseren voor RYA
- de autorisatie van een medewerker met een RYA-functie in te trekken.

Als de Autorisatiebevoegde rijbewijzen ook geautoriseerd is als RYA, kan deze ook alle RYA-werkzaamheden verrichten. Hiervoor is maar één smartcard nodig.

De geautoriseerde medewerker van het team Burgerzaken, die toegang heeft tot het rijbewijzenstation, ontvangt een persoonsgebonden smartcard (RYA) in combinatie met een persoonlijke pincode.

De medewerker tekent voor ontvangst van de persoonsgebonden smartcard en bijbehorende pincode. Deze pincode wijzigt de medewerker direct na ontvangst. Tevens wijzigt de medewerker de pincode minimaal 1x per jaar.
De persoonsgebonden smartcards en pincodes worden nooit uitgeleend of bekend gemaakt aan anderen. Persoonsgebonden smartcards worden altijd gescheiden bewaard van de pincodes en opgeborgen in een beveiligde ruimte.

De Autorisatiebevoegde rijbewijzen ziet toe op naleving hiervan.

Een medewerker met een RYA smartcard kan:
- *het backofficesysteem opstarten*
- *aanvragen scannen*
- *aanvragen goedkeuren*
- *aanvragen afwijzen*
- *aanvragen verwijderen*
- *aanvragen verzenden*
- *handmatig een nummer invoeren van onleesbare aanvragen*
- *rijbewijzen inklaren per collo*
- *inklaren per rijbewijs*
- *heraanvragen doen*
- *helpfunctie gebruiken*

De Autorisatiebevoegde rijbewijzen draagt zorg voor terugzending van de persoonsgebonden smartcards, indien deze niet meer worden gebruikt. Deze worden vergezeld van de hiertoe bestemde formulieren teruggestuurd aan de RDW.

Bijlage C: Opsomming vastgestelde procedures

Procedures met betrekking tot de BRP

Beschrijving	*vastgesteld geactualiseerd*
Procedure beoordelen van brondocumenten	31-10-2019
Procedure inschrijven in de BRP	31-10-2019
Procedure actualiseren van gegevens	31-10-2019
Procedure corrigeren van gegevens	31-10-2019
Procedure controle op volledigheid, juistheid en actualiteit gegevens	31-10-2019
Procedure verstrekkingsbeperking	31-10-2019
Procedure verstrekken van gegevens	31-10-2019
Procedure protocolleren	31-10-2019
Procedure inzagerecht in BRP	31-10-2019
Procedure terugmeldingen	31-10-2019
Procedure adresonderzoek	31-10-2019
Procedure reconstructie van data en gegevens BRP	31-10-2019

Procedures met betrekking tot reisdocumenten

Beschrijving	*vastgesteld geactualiseerd*
Procedure identiteit vaststellen en machtigen	31-10-2019
Procedure aanvragen van reisdocumenten	31-10-2019
Procedure ontvangst en transport van reisdocumenten en overige materialen	26-09-2017
Procedure bewaren en beheren van reisdocumenten en overige materialen	26-09-2017
Procedure gevonden documenten	27-07-2017
Procedure van rechtswege vervallen documenten	31-10-2019
Procedure fysieke beveiliging van het RAAS en (mobiele) aanvraagstations	27-12-2018
Procedure kasbeheer	01-12-2018

Procedures met betrekking tot rijbewijzen

Beschrijving	*vastgesteld geactualiseerd*
Procedure aanvragen van rijbewijzen	05-09-2017
Procedure verzenden van aanvragen rijbewijzen	05-09-2017
Procedure ontvangst en transport van rijbewijzen en overige materialen	05-09-2017
Procedure bewaren van rijbewijzen en overige materialen	05-09-2017
Procedure uitreiken en vernietigen van rijbewijzen	05-09-2017
Procedure bijzondere procedures rijbewijzen	27-07-2017