GEMEENTE HEUSDEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Heusden

Nr. 312273

20 december 2019

Deelbeleidsplan Informatiebeveiliging BRP en Waardedocumenten 2019 gemeente Heusden

Het college van Heusden heeft in de vergadering van 17 december 2019
besloten:

het 'Deelbeleidsplan Informatiebeveiliging BRP en Waardedocumenten 2019' en de daarbij behorende procedures vast te stellen.

Namens het college van Heusden, de secretaris,
mr. H.J.M. Timmermans

DEELBELEIDSPLAN Informatiebeveiliging BRP en Waardedocumenten

1. Algemeen
1.1. 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, burgemeester en wethouders voor de BRP respectievelijk de burgemeester[1] 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. Dit document maakt onderdeel uit van het vastgestelde Informatie beveiligingsbeleid 2019-2021 Gemeente Heusden. Het deelplan Informatiebeveiliging BRP en Waardedocumenten vormt de basis voor de uit te voeren procedures met bijbehorende formulieren en rapportages voor de BRP en Waardedocumenten.

1.2 Inleiding
BRP en Waardedocumenten zijn niet de enige bedrijfsprocessen waarvoor beveiliging noodzakelijk is en in de voornoemde wetten is voorgeschreven. De gemeente verwerkt op tal van plaatsen in de organisatie gegevens over personen, waarop de Algemene Verordening Gegevensbescherming van toepassing is. De gemeente is verplicht tot het treffen van beveiligingsmaatregelen. Ook buiten het domein van de persoonsgegevens valt er nog heel wat te beveiligen. Bijvoorbeeld besluitvormingsprocessen waarbij de gemeente Heusden als belanghebbende nadeel kan ondervinden als het besluit te vroeg in de openbaarheid komt. De Wet basisregistratie personen (Wet BRP) is de grondslag voor de basisregistratie van persoonsgegevens.

1.3 Totstandkoming, implementatie en evaluatie
1.3.1 De overleggroep Informatiebeveiliging BRP en Waardedocumenten
Ten behoeve van de totstandkoming van het plan Informatiebeveiliging BRP en Waardedocumenten is door de gemeente Heusden de overleggroep Informatiebeveiliging BRP en Waardedocumenten ingesteld.
De samenstelling hiervan is opgenomen in de bijlage Functieverdeling.
De overleggroep Informatiebeveiliging BRP en Waardedocumenten werkt onder verantwoordelijkheid van de manager Burgerzaken en de coördinatie is in handen van de beveiligingsbeheerder BRP.

De leden van de overleggroep Informatiebeveiliging BRP en Waardedocumenten hebben of een sleutelrol in het beheer van de gemeentelijke voorziening, of in het beheer van waardedocumenten, of in de (fysieke) beveiliging van het gemeentehuis.

1.3.2. Uitvoering en evaluatie
Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt en alle actoren die daarbij een rol hebben, daar op een juiste manier invulling aan geven. Beleidsdoelstellingen zijn bepalend voor het informatiebeveiligingsbeleid en in dit plan zijn die specifiek gericht op het gebied van BRP en Waardedocumenten. 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 beveiligingsfunctionaris BRP en de beveiligingsfunctionaris reisdocumenten en bij noodzaak daartoe bijgesteld. Alle medewerkers van de gemeente Heusden 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 informatiebeveiligingsbeleid, -plan, -maatregelen en/of –procedures.

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 plan Informatiebeveiliging BRP en Waardedocumenten bevat tevens een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden bezien 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 BRP en Waardedocumenten het voorliggend plan Informatiebeveiliging 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 BRP en Waardedocumenten biedt het aangepaste plan vervolgens rechtstreeks ter advisering aan betrokkenen aan. Daarna wordt het ter vaststelling aangeboden aan de bevoegde bestuursorganen, het college van B&W respectievelijk de burgemeester.

Het gehele beleid rondom BRP en Waardedocumenten dient gelijktijdig met het gemeente brede Informatiebeleid gemeente Heusden eenmaal per drie jaar te worden herijkt.

2. Informatiebeveiligingsbeleid BRP en Waardedocumenten
2.1 Informatiebeveiliging
Informatiebeveiligingsbeleid is volgens de NEN/ISO 27000 normen op schrift gesteld en door het gemeentebestuur, goedgekeurde 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 Beleidsdoelstelling Heusden
Het gemeentebestuur van Heusden 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 Heusden 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 beleidsdoelstelling wordt de eis neergelegd dat de informatiesystemen aangeduid in dit plan een beschikbaarheid tijdens werktijd kennen van minimaal 97%. Buiten werktijd worden er geen eisen gesteld aan de beschikbaarheid met uitzondering van voorzieningen in het kader van rampenbestrijding.

2.3 Wettelijk kader verwerking persoonsgegevens
De Wet BRP en de Algemene Verordening Gegevensbescherming vormen het algemeen kader voor de verwerking van persoonsgegevens.

De Autoriteit Persoonsgegevens (Ap) 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.

Het gemeentebestuur moet ook rekening houden met de beveiligingseisen die andere wetten stellen, zoals dat voor dit plan zijn de Wet BRP, de Paspoortwet en het Reglement rijbewijzen.

2.4 Taken, verantwoordelijkheden en bevoegdheden
De bestuurlijke verantwoordelijkheid voor het deel beleidsplan Informatiebeveiliging BRP en Waardedocumenten ligt bij het college van B&W respectievelijk de burgemeester. Deze organen laten het deel beleidsplan Informatiebeveiliging BRP en Waardedocumenten opstellen en zien toe op de uitvoering ervan door de betreffende medewerkers.

De beveiligingsfunctionaris BRP is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid op het gebied van de persoonsinformatievoorziening.
De beveiligingsfunctionaris BRP is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van het deel beleidsplan Informatiebeveiliging voor de gemeentelijke voorzieningen waarmee de gemeente Heusden uitvoering geef aan de Wet BRP en voor het gegevensmagazijn.

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

2.4.1 Verantwoordelijkheden gemeentebestuur
Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Heusden. Het college van B&W stelt dit deel beleidsplan Informatiebeveiliging BRP vast en de burgemeester stelt het onderdeel Waardedocumenten vast.
Genoemde bestuursorganen onderschrijven volledig de beveiligingsmaatregelen die in dit Deel-beleidsplan Informatiebeveiliging 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 deel beleidsplan Informatiebeveiliging BRP en Waardedocumenten is de rol van de beveiligingsfunctionaris BRP 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 plan Informatiebeveiliging BRP en Waardedocumenten en daarover aan het college van B&W respectievelijk de burgemeester te rapporteren.
De functie van de beveiligingsfunctionaris BRP 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.

2.4.2 Verantwoordelijkheden van het Management Team (MT)
Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle betrokken clustermanagers van de gemeente Heusden.
Het Management Team (MT) 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 plan Informatiebeveiliging BRP en Waardedocumenten
- Mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen;
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapportee
- 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.

2.4.3 Verantwoordelijkheden Chief Information Security Officer (CISO)
De taken en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn opgenomen in het Informatie beveiligingsbeleid 2019-2021 Gemeente Heusden.

2.4.4. Verantwoordelijkheden van overige rollen / functies
De verantwoordelijkheden van de rollen en/of functies van de gegevensbeheerder, privacy beheerder, applicatiebeheerder, systeembeheerder en beveiligingsbeheerder zijn vastgelegd in de Regeling beheer en Toezicht BRP.

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

2.5 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[2].
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 Heusden.

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.

2.5.1 Kwaliteitsaspecten
Informatiebeveiligingsbeleid omvat een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijke top eendrachtig duidelijk maken aan het tactisch en operationeel niveau welke gedragslijn de gemeente Heusden dient te volgen om te komen tot een adequate informatiebeveiliging. Het beleid vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Het maken en vaststellen van beveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten in een informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het Management Team (MT) 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 deze zijn nader uitgewerkt in het Informatiebeveiligingsbeleid 2019-2021 Gemeente Heusden.

2.5.1.1 Norm voor beschikbaarheid
Het college van B&W en het Management Team (MT) zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening wordt gestaakt als gevolg waarvan een aantal bedrijf kritische 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 openingstijden van het gemeentehuis 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.
De openingstijden voor publiek zijn vermeld op de website www.heusden.nl
Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt op jaarbasis tijdens kantooruren voor 97% beschikbaar te zijn.
Met kantooruren worden hier bedoeld: Maandag tot en met vrijdag van 7.00 -22.00 uur.
Aangezien de BRP in beheer is bij de landelijke overheid, is de gemeente voor de realisatie van deze norm afhankelijk van de landelijk beheerder. Voor de continuïteit in de bedrijfsvoering is het noodzakelijk dat de gemeente voorzieningen treft die onverhoopte uitval van het landelijke systeem kan opvangen. Dit betreft voorzieningen die betrekking hebben op de gegevensbestanden, netwerkverbindingen en lokale systemen.
De BRP wordt uitgevoerd met behulp van de lokale voorzieningen, die gebaseerd zijn op de Wet BRP. Voor deze voorzieningen geldt dat een uitval nooit langer mag duren dan 48 uur. Er dienen adequate voorzieningen te zijn getroffen om ook in geval van calamiteiten na maximaal 48 uur de dienstverlening aan de burger en aan andere bestuursorganen te kunnen bieden.

2.5.1.2 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 Overlijden groep 1, 1e en 6e
B	Adres groep 1, 6e
C	Relaties groep 1, 1e
D	Identificatienummers en nationaliteit groep 2, 7e groep 2, 4e groep 2, 8e
E	Overig algemeen groep 2, 9e groep 2, 5e groep 2, 2e en 3e groep 2, 10e groep 2, 11e
F	Administratief groep 3, 1e, 2e, 3e, 4e

Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens accepteert de gemeente Heusden een foutenpercentage van in totaal 5%.

2.5.1.3 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 voornoemde personen, die belast zijn met de bijhouding van BRP gegevens en/of werken met waardedocumenten dienen een geheimhoudingsverklaring te hebben ondertekend.
2.5.1.4 Norm voor controleerbaarheid
Mutaties in persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente Heusden 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 belangenverstrengeling, ook gecontroleerd moet kunnen worden wie welke mutatie heeft verwerkt. De gemeente Heusden 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.
Samenvatting
Beveiliging van (persoons-)gegevens vraagt om een zorgvuldige analyse van de risico's die met de gegevensverwerking samenhangen. Er zijn verschillende risico's te noemen die ertoe kunnen leiden dat bedrijfsprocessen stagneren. Bijvoorbeeld verlies van gegevens (raakt aan de kwaliteitsaspecten integriteit en beschikbaarheid) en onrechtmatig gebruik van gegevens (raakt aan het aspect vertrouwelijkheid), maken de resultaten van bedrijfsprocessen onbetrouwbaar. De in het voorliggend Deelbeleidsplan Informatiebeveiliging 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 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 deze wet voorschrijft. De AVG 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 AVG. Bovendien geldt op grond van artikel 4.3 wet BRP de verplichting om jaarlijks uiterlijk op 31 december zelf onderzoek te doen naar de inrichting, de werking en de beveiliging van de basisregistratie, 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, 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 plan Informatiebeveiliging 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.
Periodieke zelfevaluatie, onderzoek en accountantscontrole

3.2.1 Zelfevaluatie
De in het plan Informatiebeveiliging 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.
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 login. 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 BPR via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt. De vragenlijst moet jaarlijks vóór 31 december definitief zijn ingevuld. De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsfunctionaris BRP 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 31 december naar de Rijksdienst voor Identiteitsgegevens.

De beveiligingsfunctionaris BRP 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 het agentschap BPR. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks vóór 31 december definitief zijn ingevuld. De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsfunctionaris reisdocumenten en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan 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, privacy beheer, 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 het cluster Klantcontactcentrum door kwaadwillende 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
- Beheer
- Uitreiking

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 Heusden bereikt doordat op het uitreikformulier of 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 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. Zie procedure Ontbreken van voldoende functiescheiding.
  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.

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 Heusden bereikt doordat op het uitreikformulier of 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.
Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Zie procedure Ontbreken van voldoende functiescheiding.
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.

[1]In het vervolg van dit document zal voor de beide organen de term ‘gemeentebestuur’ worden gebezigd met uitzondering van die plaatsen waar het strikt noodzakelijk is om de bestuursorganen concreet te duiden.
[2]Richtsnoeren beveiliging van persoonsgegevens, Cbp 2013 februari 2013