Gemeente Etten-Leur

Informatiebeveiligingsplan basisregistratiepersonen en waardedocumenten

Inhoudsopgave

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 deel uit van het in de vorige zin bedoelde informatiebeveiligingsplan en vormt de basis voor de uit te voeren procedures met bijbehorende formulieren en rapportages waarnaar wordt verwezen in het hoofdstuk bijlagen.

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, waarvoor de AVG in artikel 32 de gemeente Etten-Leur verplicht tot het treffen van beveiligingsmaatregelen.

Een gemeentebreed beveiligingsbeleid met daarop afgestemde plannen is noodzakelijk om de totale bedrijfsvoering van de gemeente Etten-Leur te beveiligen. Dit plan staat op zichzelf, maar is voor wat betreft de algemene beveiligingsmaatregelen afgestemd op de inhoud van de Baseline Informatiebeveiliging Nederlandse gemeenten van KING (mei, 2013 NEN-ISO/IEC 27002:2007).

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

[1] In het vervolg van dit document zal voor de beide organen de term 'gemeentebestuur' worden gebruikt met uitzondering van die plaatsen waar het strikt noodzakelijk is om de bestuursorganen concreet te duiden.

1.3 Totstandkoming, implementatie en evaluatie

1.3.1 Informatiebeveiliging BRP

Ten behoeve van de totstandkoming van het informatiebeveiligingsplan BRP en Waardedocumenten is er periodiek overleg tussen privacybeheerder BRP, beveiligingsfunctionaris reisdocumenten, kwaliteitsbeheerder BRP en informatiebeheerder BRP.

De leden van overleggroep informatiebeveiliging BRP hebben of een sleutelrol in het beheer van de gemeentelijke voorziening, of in het beheer van waardedocumenten, of in de (fysieke) beveiliging van het stadhuis.

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 teamleden verantwoordelijkheden krijgen voor de implementatie van dit beleid.

De teamleden worden betrokken (o.a. tijdens werkoverleg) bij de ontwikkeling en implementatie van het beleid en zijn mede verantwoordelijk voor de uitvoering.

Dit plan wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de kwaliteitsbeheerder BRP en bij noodzaak daartoe bijgesteld. Alle teamleden van de gemeente Etten-Leur 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 teamleden rechtstreeks gecommuniceerd.

Dit informatiebeveiligingsplan 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 overleggroep informatiebeveiliging BRP het voorliggend informatiebeveiligingsplan BRP en Waardedocumenten en de daarbij behorende procedures en bijlagen

jaarlijks opnieuw bekijkt op actualiteit en controleert op naleving van de beleidsuitgangspunten.

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

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

1.4 Verantwoording

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

Dit informatiebeveiligingsplan BRP en Waardedocumenten is afgestemd met de inhoud van de Baseline Informatiebeveiliging Nederlandse gemeenten voor Nederlandse Gemeenten (BIG) van KING.

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

1.5 Goedkeuring

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

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

Etten-Leur, 02-10-2018

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

Wnd secretaris, De burgemeester,

C.M. Martens Mw. M.W.M. de Vries

Burgemeester in zijn hoedanigheid als verantwoordelijke voor het onderdeel Waardedocumenten.

De burgemeester,

Mw. M.W.M. de Vries

2 Informatiebeveiligingsbeleid

2.1 Informatiebeveiligingbeleid

Het informatiebeveiligingbeleid is in een apart document vastgesteld (IB Beleid 2017-2020) en wordt jaarlijks getoetst op actualiteit.

2.2 Beleidsdoelstelling Etten-Leur

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 98,0%. 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

Buiten het algemeen kader van de AVG dient het gemeentebestuur ook rekening te houden met de beveiligingseisen die andere wetten stellen, zoals dat voor dit plan zijn de Wet BRP, de Paspoortwet (paspoortuitvoeringsregeling) en het Reglement rijbewijzen.

2.4 Taken, verantwoordelijkheden en bevoegdheden

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

De security officer is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid op het gebied van de persoonsinformatievoorziening en voor het gegevensmagazijn.
De kwaliteitsbeheerder BRP is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van het informatiebeveiligingsplan voor de gemeentelijke voorzieningen waarmee de gemeente Etten-Leur uitvoering geef aan de Wet BRP.

Beveiligingsfunctionaris reisdocumenten en overleggroep Informatiebeveiliging BRP en waardedocumenten is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van het informatiebeveiligingsplan BRP en Waardedocumenten en ziet erop toe dat eens per jaar gecontroleerd wordt of de nog te nemen maatregelen gerealiseerd zijn (zie Regeling Beheer en Toezicht BRP).

2.4.1 Verantwoordelijkheden gemeentebestuur

Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Etten-Leur. Het college van B&W stelt

dit informatiebeveiligingsplan BRP vast en de burgemeester stelt het onderdeel Waardedocumenten vast.

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

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

De beveiligingsfunctionaris reisdocumenten en overleggroep BRP en waardedocumenten dragen zorg voor een jaarlijkse evaluatie en bijstelling van het informatiebeveiligingsplan BRP en Waardedocumenten. Deze hebben de verantwoordelijkheid om namens de bestuursorganen toe te zien op naleving van de beveiligingsmaatregelen en –procedures zoals uitgewerkt in het informatiebeveiligingsplan BRP en Waardedocumenten en daarover aan het college van B&W respectievelijk de burgemeester te rapporteren.

2.4.2 Verantwoordelijkheden van het Management Team

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van De secretaris / algemeen directeur en de afdelingshoofden, zij vormen samen het managementteam. Daarnaast is de lijnverantwoordelijkheid belegd bij de respectievelijke proceseigenaren (meestal de teamleiders).

Het Management Team bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

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

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

2.4.3 Verantwoordelijkheden van overige rollen / functies

De verantwoordelijkheden van de rollen en/of functies zijn vastgelegd in de bijlagen (governance) behorende bij het persoonsinformatiebeleid 2017-2020.

2.5 Passende technische en organisatorische maatregelen

Dit is reeds opgenomen in het informatiebeveiligingsbeleid van de gemeente Etten-Leur.

De gemeente Etten-Leur hanteert voor deze kwaliteitsaspecten de volgende normen:

2.5.1.1 Norm voor beschikbaarheid

Het college van B&W en het Centraal Management Team zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening wordt gestaakt als gevolg waarvan een aantal bedrijfskritische applicaties niet meer kunnen functioneren. Dit geldt onder andere en in het bijzonder voor de informatievoorziening vanuit de BRP.
De informatievoorziening met betrekking tot de BRP moet tijdens de openingstijden van het stadhuis permanent beschikbaar zijn. In cijfers uitgedrukt betekent dit op jaarbasis een beschikbaarheid van gemiddeld 97,0%.

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

maandag : 09.00 tot 19.00 uur

dinsdag tot en met vrijdag : 09.00 tot 17.00 uur

Tevens is ons digitaal loket altijd geopend. Hoewel onderbrekingen (storingen / werkzaamheden) hier doorgaans een lagere impact hebben, is de beschikbaarheid van het digitaal loket belangrijk.

Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt op jaarbasis tijdens kantooruren voor 98,0% beschikbaar te zijn.

Met kantooruren worden hier bedoeld: 07:00 - 19:00.

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 eerstkomende jaren zal de BRP nog worden uitgevoerd met behulp van de lokale voorzieningen, die gebaseerd zijn op de Wet GBA. Voor deze voorzieningen geldt dat een uitval nooit langer mag duren dan 48 uur. Er dienen adequate voorzieningen te zijn getroffen om ook in geval van

calamiteiten na maximaal 48 uur de dienstverlening aan de burger en aan andere bestuursorganen in te kunnen voorzien.

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:

Groep (art 21 Regeling BRP) Omschrijving	Klasse	Norm
1. Algemene Gegevens	A. Persoon en Overlijden	99,70 %
(Burgerlijke Staat)	B. Adres	99,70 %
	C. Relaties	99,60 %
Totaal Groep 1		
2. Algemene Gegevens	D. Identificatienummers en nationaliteit	99,50 %
(overig)	E. Overig algemeen	99,50 %
Totaal Groep 2		
3. Administratieve Gegevens	F. Administratief	99,40 %
Totaal Groep 3		

Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens accepteert de gemeente Etten-Leur een foutenpercentage zoals deze vermeld is in de kwaliteitsmonitor.
Daarnaast is het van belang dat de gegevens die over iemand zijn opgenomen in de BRP overeenkomen met de werkelijkheid. Om die reden wordt er fors geïnvesteerd in de voorkoming van dergelijke fouten, bijvoorbeeld door adrescontroles uit te voeren, versterking van de samenwerking met ketenpartners en door actief in te zetten op preventie en bestrijding van fraude.

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 ambtseed en geheimhoudingsverklaring te hebben ondertekend en een recente VOG te overleggen.

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 Etten-Leur 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 Etten-Leur 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.

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 de wet voorschrijft. Dit houdt in dat de volgende beveiligingsmaatregelen van toepassing zijn (artikel 32 AVG en artikel 6 Besluit BRP):

Artikel 32

Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

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.

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.

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 dit informatiebeveiligingsplan BRP en Waardedocumenten verder uitgewerkt in concrete voorschriften op het gebied van fysieke beveiliging, back-up en herstel en enkele voorschriften over hoe te handelen in bepaalde situaties. Artikel 93 lid 1 PUN vereist daartoe organisatorische maatregelen.

3.1.3 Rijbewijzen

Het uitgifteproces van rijbewijzen komt sinds enkele jaren sterk overeen met dat van de Reisdocumenten.

De artikelen 122 tot en met 130 van het Reglement Rijbewijzen hebben betrekking op de eisen aan de beveiliging rondom de uitgifte van

rijbewijzen. Zo wordt geëist dat de met afgifte van rijbewijzen belaste autoriteiten zorg dragen voor een op schrift gestelde beveiligingsprocedure, met daarin in ieder geval beveiligingsvoorschriften ten aanzien van: toegang van personen tot en het beheer van rijbewijzen, de met de afgifte van rijbewijzen verband houdende materialen, apparatuur, toegangspassen en gebruikerscodes tot de apparatuur, de verantwoordelijkheden van de beveiligingsfunctionaris en de functiescheiding.

3.2 Periodieke zelfevaluatie, onderzoek en accountantscontrole

3.2.1 Zelfevaluatie

De in het informatiebeveiligingsplan BRP en Waardedocumenten voorgestelde beveiligingsmaatregelen en –procedures vormen voor een groot deel eens per jaar het object van onderzoek bij de door de Paspoortwet en Wet BRP voorgeschreven zelfevaluaties Paspoorten en NIK en BRP.
De uitslagen van deze zelfevaluaties worden door het college van B&W voor de BRP en de burgemeester voor de Reisdocumenten naar de Rijksdienst voor Identiteitsgegevens (RvIG) gezonden en openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. Die kwaliteitsmonitor is er ook voor de controle op de inhoudelijke kwaliteit van de gegevens.

3.2.2 Onderzoek BRP gegevens

De Rijksdienst voor Identiteitsgegevens voert periodiek inhoudelijke kwaliteitscontroles uit op de gegevens in de landelijke voorziening voor de BRP en stelt de resultaten van die controles beschikbaar via de Kwaliteitsmonitor. Elke gemeente kan de resultaten van de op haar betrekking hebbende onderdeel van de BRP in het onderdeel 'monitor Gegevens' van de Kwaliteitsmonitor bekijken met behulp van een persoonlijke log-in. De gegevens in de BRP moeten voldoen aan de kwaliteitsnormen, welke op grond van artikel 47 Besluit BPR bij Ministeriële regeling worden bepaald.

3.2.2 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 RvIG 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 beveiligingscoördinator en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan de het college van

B&W. Deze ondertekent de rapportage en stuurt deze vóór 14 februari naar de Rijksdienst voor Identiteitsgegevens.

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

3.2.2 Onderzoek Paspoorten en NIK

Sinds april 2013 gebruiken gemeenten voor haar onderzoek naar reisdocumentenproces de vragenlijst in de Kwaliteitsmonitor van de Rijksdienst voor Identiteitsgegevens. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks vóór 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 de het college van B&W. Het bestuursorgaan, de burgemeester, ondertekent de rapportage en stuurt deze vóór 14 februari 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.

3.2.3 Accountantscontrole Rijbewijzen

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

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

3.3 Taken, verantwoordelijkheden en bevoegdheden

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

Op het gebied van de Waardedocumenten zijn aangewezen een beveiligingsfunctionaris reisdocumenten en rijbewijzen, de Autorisatie Bevoegde Reisdocumenten en rijbewijzen

De beschrijving en toekenning van de rollen in het kader van de Waardedocumenten maken deel uit van de bijlagen (governance)

3.4 Functiescheiding Waardedocumenten

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

Hieronder een korte uitleg van de relevante termen:

- Aanvraag/verstrekking: Hieronder wordt verstaan het bij de balie behandelen van een aanvraag voor een waardedocument en de beslissing daarop. Bij de aanvraag van een rijbewijs dient een aanvraagformulier te worden ingevuld; bij de aanvraag van een reisdocument moet een foto- en handtekeningformulier worden gebruikt. Eventueel kan daarbij een aanvraagformulier worden ingevuld.
- Beheer: Hieronder wordt verstaan de verantwoordelijkheid voor de materialen en (gepersonaliseerde) waardedocumenten tussen het moment van de aanvraag en de uitreiking.
- Uitreiking: Hieronder wordt verstaan het feitelijk aan de houder ter beschikking stellen van het op zijn naam gestelde waardedocument.

3.4.1 Functiescheiding Reisdocumenten

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

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

De functiescheiding op dit gebied wordt in de gemeente Etten-Leur bereikt doordat op het uitreikformulier of het aanvraagformulier de paraaf van het teamlid is geplaatst, die over de aanvraag heeft beslist.

- Door de teamleden wordt er middels de signalering in de reisdocumentenmodule op toegezien dat de uitreiking door een andere teamlid 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 teamleden 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 teamleden, 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 ander teamlid uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

De functiescheiding op dit gebied wordt in de gemeente Etten-Leur bereikt doordat op het uitreikformulier of het aanvraagformulier de paraaf van het teamlid is geplaatst, die over de aanvraag heeft beslist. Door de teamleden wordt er middels de signalering in de rijbewijsmodule op toegezien dat de uitreiking door een andere teamlid 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 beveiligingscoördinator rijbewijzen of de schriftelijke vastlegging aanwezig is en de aanvraag, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

4 Bijlagen

Algemeen
Risico inventarisatie en evaluatie BRP

Procedure Antecedentenonderzoek
Procedure Introductie nieuw personeel
Procedure Clear-desk policy
Procedure Communicatie over beveiliging
Procedure Rapportage van Incidenten
Procedure Sleutel- en toegangsbeheer
Procedure Toegangsbeleid gemeentelijke gebouwen en ruimten

Rapportage Controle communicatie over beveiliging
Rapportage Evaluatie informatiebeveiligingsbeleid en beveiligingsplan
Rapportage Toetsing Clear-desk policy

Bijlage Functieverdeling

ICT
Procedure Autorisatie tot het lokale netwerk

Rapportage Controle autorisaties LAN
Rapportage test restore back-up
Rapportage uitwijk

Bijlage Back-up registratie

BRP
Regeling Beheer en Toezicht BRP

Procedure Adresonderzoek
Procedure Autorisatie tot de gemeentelijke voorziening
Procedure Correctie
Procedure Gegevensverwerking
Procedure Herstel van mutaties
Procedure Identificatie en Machtiging
Procedure Inzagerecht
Procedure Protocollering
Procedure Terugmeldingen
Procedure Verstrekkingsbeperking
Procedure Verstrekken gegevens uit de BRP
Procedure Verstrekking van gegevens aan organen van de gemeente

Rapportage Controle autorisaties
Rapportage Controle inzagerecht
Rapportage Controle gegevensverstrekking en protocollering
Rapportage Controle gegevensverwerking
Rapportage Controle privacyregelgeving
Rapportage Controle recht op verstrekkingsbeperking
Rapportage Evaluatie en beveiligingsbeleid en plan
Rapportage Terugmeldingen
Rapportage Test herstel mutaties

Bijlage Activiteitenkalender informatiebeveiliging en privacy
Bijlage Autorisatieformulier BRP
Bijlage formulier registratie reconstructie
Bijlage Geheimhoudingsverklaring
Bijlage Parafenlijst inzage

Waardedocumenten
Procedure Aanvraag en uitreiking waardedocumenten
Procedure Autorisatie RAAS aanvraagstations en rijbewijsmodule
Procedure Back-up en restore RAAS
Procedure Kasbeheer
Procedure Ontbreken van voldoende functiescheiding
Procedure Ontvangst en beheer waardedocumenten
Procedure Overvalinstructie en agressief publiek

Rapportage Controle autorisaties RAAS/Aanvraagstations en rijbewijsmodule
Rapportage Controle ontbreken van voldoende functiescheiding
Rapportage Evaluatie Paspoorten en NIK
Rapportage Evaluatie rijbewijzen

Bijlage Aangewezen teamleden waardedocumenten
Bijlage Aangifteformulier overval

Bijlage Activiteitenkalender Waardedocumenten
Bijlage Autorisatiebevoegden waardedocumenten
Bijlage Formulier Identificerende vragen
Bijlage Functies Waardedocumenten
Bijlage Ontvangst- en innamebewijs identificatiekaart/smartcard
Bijlage Ontvangstlijst waardedocumenten
Bijlage Onvoldoende functiescheiding