Gemeente Oostzaan

GEMEENTEBLAD

Officiële uitgave van de gemeente Oostzaan

Nr. 189224

30 juli 2019

Besluit van het college van burgemeester en wethouders en de burgemeester van de gemeente Oostzaan houdende regels omtrent beveiliging BRP en waardedocumenten (Beveiligingsrichtlijnen BRP en waardedocumenten 2019)

Beveiligingsrichtlijnen BRP en waardedocumenten Oostzaan 2019

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 dienen jaarlijks te rapporteren over de mate waarin en de wijze waarop wettelijke regelgeving wordt gehandhaafd. Aan de getroffen beveiligingsmaatregelen dienen richtlijnen aangaande informatiebeveiliging ten grondslag te liggen. De uitgangspunten en beveiligingsprocedures die invulling aan de gestelde eisen moeten geven zijn in deze richtlijnen opgenomen. Dit document maakt onderdeel uit van het vastgestelde Informatiebeveiligingsbeleid en vormt de basis voor de uit te voeren procedures. De bijbehorende formulieren en rapportages waarnaar wordt verwezen, zijn terug te vinden in het hoofdstuk 'Bijlagen'.

Inleiding
Op basis van de Algemene Verordening Gegevensbescherming (AVG) is de Gemeente Oostzaan 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 gemeentebreed informatiebeveiligingsbeleid met daarop afgestemde plannen is vastgesteld om de totale bedrijfsvoering van de gemeente Oostzaan te beveiligen. Deze richtlijnen bevatten specifieke maatregelen, maar is voor wat betreft algemene beveiligingsmaatregelen afgestemd op de inhoud van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), opgesteld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

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 plaatsonafhankelijke dienstverlening aan burgers te kunnen verlenen.

Totstandkoming, implementatie en evaluatie
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 beveiligingsbeheerder (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 beveiligingsbeheerder (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 Oostzaan worden via de gebruikelijke interne kanalen geïnformeerd over wijzigingen binnen het informatiebeveiligingsbeleid, de richtlijnen BRP en waardedocumenten en aanpassingen binnen maatregelen of procedures omtrent informatiebeveiliging. 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.

De informatiebeheerder biedt de aangepaste richtlijnen vervolgens rechtstreeks ter kennisgeving aan het managementteam aan. Daarna wordt het ter vaststelling aangeboden aan de bevoegde bestuursorganen, het college van B en W respectievelijk de burgemeester.

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

Beleidsuitgangspunten

Informatiebeveiliging
Het geldende informatiebeveiligingsbeleid is opgesteld volgens de voorgeschreven Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) normen en vervolgens door het gemeentebestuur, de gemeentesecretaris en het managementteam goedgekeurd voor toepassing op de beveiliging van informatievoorzieningen.

Onder informatiebeveiliging wordt in dit kader verstaan: een samenhangend geheel van maatregelen die de beschikbaarheid, vertrouwelijkheid en integriteit van gegevens garanderen en de controleerbaarheid van de toepassing van de uitgevoerde werkzaamheden mogelijk maakt.

Raakvlakken met ander beleid
Het informatiebeveiligingsbeleid heeft raakvlakken met het beleid en de daaruit voortvloeiende procedures, 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' (ook wel 'clean desk policy' genoemd).

Beleidsdoelstelling
Als concrete norm voor de realisering van de beleidsdoelstellingen wordt de eis neergelegd dat de informatiesystemen zoals aangeduid in dit plan, tijdens reguliere werktijden voldoen aan de beschikbaarheidseis van minimaal 95%. Buiten reguliere werktijden worden er geen eisen gesteld aan de beschikbaarheid van de systemen met uitzondering van voorzieningen die in het kader van rampenbestrijding zijn getroffen.

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:

- Organisaties moeten 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.

Taken, verantwoordelijkheden en bevoegdheden
De bestuurlijke verantwoordelijkheid voor de richtlijnen Informatiebeveiliging 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 is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid op het gebied van de persoonsinformatievoorziening.

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

De beveiligingsbeheerder (CISO) 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).

Verantwoordelijkheden gemeentebestuur
Beveiliging op bestuurlijk niveau betreft de verantwoordelijkheid van het college van B en W van de gemeente Oostzaan. Het college van B en W stelt deze richtlijnen vast en de burgemeester draagt zorg voor het onderdeel waardedocumenten.

Genoemde bestuursorganen onderschrijven de beveiligingsmaatregelen die in deze richtlijnen 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 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 de richtlijnen BRP en waardedocumenten en daarover aan het college van B en W respectievelijk de burgemeester te rapporteren.

De functie van 'de beveiligingsbeheerder' moet niet verward worden met de functie van ‘beveiligingsfunctionaris waardedocumenten’. Deze functie kent zeer specifieke taken en verantwoordelijkheden op het gebied van enerzijds de beveiliging van reisdocumenten en anderzijds de beveiliging van rijbewijzen. Zie Aanwijzing beheerfunctionarissen Regeling Beheer en Toezicht

Verantwoordelijkheden van het managementteam
Beveiliging op ambtelijk niveau, betreft de verantwoordelijkheid van alle leden van het management van OVER-gemeenten. Het management 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 van de realisatie van beveiligingsmaatregelen zoals beschreven in de richtlijnen BRP en waardedocumenten, gerapporteerd door de beveiligingsbeheerder.
- Het benoemen van mogelijke ontwikkelingen die de bedrijfsinformatie kunnen bedreigen.
- De bespreking van en het toezicht op beveiligingsincidenten, zoals gerapporteerd door de beveiligingsfunctionaris reisdocumenten 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.

Verantwoordelijkheden Chief Information Security Officer (Beveiligingsbeheerder)
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 gemeentebrede Informatiebeveiligingbeleid;
- de voortgang en de realisatie van beveiligingsmaatregelen zoals beschreven in de richtlijnen;
- het actualiseren van het gemeentebreed 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 Oostzaan 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 Oostzaan.

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

Voor alle in de beveiligingsrichtlijnen BRP en waardedocumenten voorkomende functies is in de Aanwijzing beheerfunctionarissen Regeling Beheer en Toezicht de vervanging vastgelegd.

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 Oostzaan.

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.
- De stand van de techniek.
- De kosten van de te treffen maatregelen.

Kwaliteitsaspecten
Het Informatiebeveiligingsbeleid omvat een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijke top eendrachtig duidelijk maken aan het tactisch en operationeel niveau welke gedragslijn de gemeente Oostzaan 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 biedt nog geen garantie voor een goede werking. Hiervoor is het nodig dat de uitgangspunten in het Informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het managementteam vast te stellen of de maatregelen werken. Evaluatie van het beleid dient vervolgens plaats te vinden om na te gaan of het beleid nog steeds aansluit op de organisatie en of de juiste maatregelen zijn getroffen.

De beveiliging van persoonsgegevens kent vier kwaliteitsaspecten, namelijk:

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

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

3: **Vertrouwelijkheid.** Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.

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

De gemeente Oostzaan hanteert voor deze kwaliteitsaspecten de volgende normen:

Norm voor beschikbaarheid
Het college van B en W en het managementteam zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te staan als de informatievoorziening wordt gestaakt en een aantal bedrijfskritische applicaties niet meer 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 95%.

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

Iedere werkdag van maandag, dinsdag en woensdag van 08:45 uur tot 17:00 uur op afspraak, woensdag van 08:30 uur tot 19:00 uur op afspraak en de vrijdag van 08:45 uur tot 12:00 uur op afspraak .

Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt tijdens kantooruren, een jaarlijks gemiddelde van 95% te handhaven.

Met kantooruren worden hier bedoeld: maandag tot en met vrijdag van 07:00 uur tot 19:00 uur.

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 bedrijfsvoering is het noodzakelijk dat de gemeente voorzieningen treft, die onverhoopte storingen binnen het landelijke systeem kunnen opvangen. Dit betreft voorzieningen die betrekking hebben op de gegevensbestanden, netwerkverbindingen en lokale systemen.

De eerstkomende jaren zal de BRP nog worden uitgevoerd met behulp van de lokale voorzieningen die gebaseerd zijn op de Wet GBA. Voor deze voorzieningen geldt dat een uitval nooit langer mag duren dan 48 uur. Er dienen adequate voorzieningen te zijn getroffen om ook in geval van calamiteiten, na maximaal 48 uur de dienstverlening aan de burger en aan andere bestuursorganen te kunnen hervatten.

Norm voor integriteit
De technische en organisatorische inrichting van de gemeentelijke informatiesystemen zijn zodanig van aard en opzet, dat de gegevens daarbinnen volledig, juist, en actueel zijn. De verantwoordelijke personen en afdelingen binnen de gemeentelijke organisatie treffen de benodigde maatregelen om dit zeker te stellen.

Het is niet te voorkomen dat gegevens fouten bevatten. Een BRP-bestand zonder fouten is een nobel streven, maar het is niet realistisch om dit als concrete eis te stellen. Ten behoeve van het evaluatie instrument zijn kwaliteitsindicatoren opgesteld 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 wordt onderscheid gemaakt tussen zes klassen:

Klasse	**Omschrijving**	**Norm**
A	Persoon en Overlijden groep 1, 1 e en 6e	99,7%
B	Adres groep 1, 6e	99,7%
C	Relaties groep 1, 1e	99,6%
D	Identificatienummers en nationaliteit groep 2, 7e groep 2, 4e groep 2, 8e	99,5%
E	Overig algemeen groep 2, 9e groep 2, 5e groep 2, 2 e en 3e	99,5%

	groep 2, 10e groep 2, 11e	
F	Administratief groep 3, 1 e, 2 e, 3 e, 4e	99,4%

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

Norm voor vertrouwelijkheid
Uitsluitend bevoegde personen in dienst van of werkzaam ten behoeve van de gemeente Oostzaan hebben toegang tot en kunnen bij de uitvoer van hun taken, gebruik maken van de in de voor hen relevante registraties opgenomen gegevens. De bevoegdheid van een persoon moet worden afgeleid van diens taak, dit ter beoordeling van de beheerder van de betreffende registratie, op aangeven van de direct leidinggevende van deze persoon. Degenen van de voornoemde personen, die belast zijn met de registratie van BRP gegevens of werken met waardedocumenten, dienen een geheimhoudingsverklaring te hebben ondertekend.

Norm voor controleerbaarheid
Mutaties van persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente reiken. Toelating tot Nederland is bijvoorbeeld mede afhankelijk van de nationaliteit van de aanvrager. Hoogte en duur van uitkeringen zijn veelal afhankelijk van leeftijd en de burgerlijke staat. Dat betekent niet alleen dat de kwaliteit van de geregistreerde gegevens hoog dient te zijn, maar lettend op mogelijke belangenverstrengeling dient er ook gecontroleerd te kunnen worden wie welke mutatie heeft verwerkt. De gemeente Oostzaan kent als norm dat 99% van alle mutaties van persoonsgegevens herleidbaar moet zijn naar de individuele persoon die daarvoor verantwoordelijk was. De norm op het gebied van de controleerbaarheid van raadplegingen is hiervoor vastgesteld op 90%.

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 voorliggende richtlijnen BRP en waardedocumenten opgenomen procedures hebben als doel te voorkomen, dat de risico's uit de aan verwerking van persoonsgegevens verbonden risicoklasse (II) zich voordoen. Uitvoering van de procedures maakt het bedrijfsproces controleerbaar uit oogpunt van beveiliging.

BRP en waardedocumenten

Wettelijk kader

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.

Als grondslag voor het beveiligingsbeleid op het onderdeel BRP in deze richtlijnen 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.*

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 de richtlijnen 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.

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

Periodieke zelfevaluatie, onderzoek en accountantscontrole
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 Identiteitsgegevens gezonden en openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. De Kwaliteitsmonitor is ook voor de controle op de inhoudelijke kwaliteit van de gegevens.

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

Onderzoek BRP processen
Gemeenten moeten periodiek zelf onderzoeken of zij voldoen aan de eisen die de wetgever stelt op het gebied van beveiliging en privacy bij de uitvoering van de BRP-werkzaamheden. Deze controle voert de gemeente uit aan de hand van een digitale vragenlijst BRP die de Rijksdienst Identiteitsgegevens via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt. De vragenlijst moet jaarlijks 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 Identiteitsgegevens toe.

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

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 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.

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 vijf jaar bewaard. Op de eventueel geconstateerde tekortkomingen wordt actie ondernomen.

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 reisdocumenten, de beveiligingsfunctionaris rijbewijzen en de autorisatiebevoegde 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 'Aanwijzing van beheerfunctionarissen' de vervanging vastgelegd.

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

Hieronder een korte uitleg van de relevante termen:

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

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.
- 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 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 waardedocumenten of de schriftelijke vastlegging aanwezig is van de aanvraag/verstrekking, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

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

Functiescheiding 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 Oostzaan bereikt doordat op het uitreikingsformulier 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 functiescheiding.

Hierbij gelden op grond van artikel 128, lid 3 van het Reglement rijbewijzen de volgende voorschriften:

Schriftelijk wordt vastgelegd:

- wat de reden is er tijdelijk niet aan de eis van functiescheiding kan worden voldaan;
- binnen welke periode er niet aan de eis van functiescheiding kan worden voldaan.
- wat de namen zijn van de ambtenaren, die in deze periode zijn belast met de aanvraag, het beheer en de uitreiking van 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 reis en waardedocumenten of de schriftelijke vastlegging aanwezig is en de aanvraag, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

Inwerkingtreding en citeertitel

1. Deze regeling treedt in werking met ingang van de dag na de dag van haar bekendmaking.
2. Gelijktijdig met de inwerkingtreding van deze regeling wordt de regeling Informatiebeveiliging BRP en Waardedocumenten vastgesteld op 16 september 2014 ingetrokken.
3. Deze regeling kan worden aangehaald als: Beveiligingsrichtlijnen BRP en waardedocumenten 2019.

Goedkeuring

Ter bekrachtiging van het voorliggende richtlijnen Informatiebeveiliging BRP en waardedocumenten aldus besloten te Oostzaan in de vergadering van 18 juni 2019.

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

de gemeentesecretaris,
A. van den Assem

de burgemeester,
R. Meerhof

Burgemeester in zijn hoedanigheid verantwoordelijke voor het onderdeel Waardedocumenten.

Burgemeester,
R. Meerhof