gemeente Oosterhout

Informatiebeveiligingsplan BRP en Waardedocumenten

Gemeente Oosterhout 2025

Informatiebeveiligingsplan BRP en Waardedocumenten 2025

Versie	Datum	Auteur	Status	Opmerkingen
0.1	31-08-2024		Review	Grondige review, specifiek gemaakt voor BRP en waarde documenten verwijzing naar algemeen informatiebeveiligingsbeleid

(Beveiligingsbeheerder BRP – Reisdocumenten & Rijbewijzen)

Oosterhout, 31-08-2024

Inhoudsopgave

1 Algemeen

1.1 Algemeen

De wetgever stelt in de Wet Basisregistratie Personen (Wet BRP), de Paspoortwet en het Reglement Rijbewijzen eisen aan de beveiliging van de uitvoeringsprocessen voor de basisregistratie personen (BRP) en waardedocumenten (paspoorten, identiteitsbewijzen en rijbewijzen). De verantwoordelijke bestuursorganen, burgemeester en wethouders voor wat betreft de BRP en de burgemeester ten aanzien van waardedocumenten[1], 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 Informatiebeveiligingsplan BRP en Waardedocumenten is een aanvulling op het gemeente brede informatiebeveiligingsbeleid en vormt de basis voor uit te voeren procedures met bijbehorende formulieren en rapportages.

1.2 Inleiding

De BRP en waardedocumenten zijn niet de enige bedrijfsprocessen waarvoor beveiliging noodzakelijk is en in wetten is voorgeschreven.
De gemeente verwerkt op tal van plaatsen in de organisatie gegevens over personen, waarvoor de Algemene Verordening Gegevensbescherming (AVG) in o.a. artikel 5 en 32 de gemeente verplicht tot het treffen van beveiligingsmaatregelen.

1.3 Samenhang met informatiebeveiligingsbeleid gemeentebreed

Het college heeft het beveiligingsbeleid Gemeente Oosterhout in 2022 vastgesteld. Het in dit strategisch beleidsdocument gedefinieerde doel is voldoen aan wet- en regelgeving. Hierbij wordt het normenkader van de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd. In dit normenkader zijn te treffen maatregelen op hoofdlijnen opgenomen. In de technische en algemene informatiebeveiligingsbeleidsdocumenten zijn de algemeen te treffen beveiligingsmaatregelen opgenomen. Specifiek voor de activiteiten en verplichtingen die voortvloeien uit de Wet BRP en/of de verwerking van waardedocumenten zijn deze beveiligingsmaatregelen in dit document opgenomen en uitgewerkt.

(PUN: Paspoortuitvoeringsregeling Nederland 2001, PNIK: Paspoort Nationaal en Nederlandse Identiteitskaart). Voor de uitvoering van de Wet BRP en verwerking van waardedocument ziet de beveiligingsfunctionaris PUN/PNIK toe op de operationele invulling van de informatiebeveiliging. De volgende taken zijn hierbij van belang:

- Signaleren van wijzigingen op het gebied van informatiebeveiliging mbt BRP en PNIK informatiebeveiligingsbeleid.
- Uitvoeren van controles van de uitgevoerde werkzaamheden rondom BRP en waarde documenten.
- Rapporteren over de uitgevoerde controles en hieruit voortkomende bevindingen.
- Bewaken van benodigde acties die uit de controles naar voren zijn gekomen.

[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.

1.4 Beveiligingsbeleid BRP en waardedocumenten

De Wet BRP is de grondslag voor de basisregistratie van persoonsgegevens.

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt en alle factoren die daarbij een rol hebbendaar 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 de 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 beveiligingsbeheerder worden vastgesteld of de maatregelen worden nageleefd.

Dit plan wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de informatiebeveiligingsbeheerder en bij noodzaak daartoe bijgesteld. Alle bij de uitvoering van de BRP en waardedocumenten betrokken medewerkers van de gemeente Oosterhout worden via het reguliere werkoverleg geïnformeerd over voor hen van belang zijnde wijzigingen in informatiebeveiligingsbeleid, -plan, -maatregelen en/of –procedures. Hierbij draagt de leidinggevende het belang van het volgen van dit beleid uit en dient als promotor hiervan.

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

Dit informatiebeveiligingsplan 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 de BRP en waardedocumenten.

1.5 Verantwoording

Voor de verantwoording aan het rijk en gemeenteraad wordt de ENSIA zelfevaluatie gebruikt. Hiermee wordt de stand van zaken rondom de BRP en waardedocumenten aan de Rijksdienst voor Identiteit Gegevens (RvIG) de Autoriteit Persoonsgegevens (AP) en het college van burgemeester en wethouders gerapporteerd. Binnen de P&C-cyclus wordt in het jaarverslag onder de paragraaf Bedrijfsvoering gerapporteerd over de stand van zaken m.b.t. de integrale informatiebeveiliging en privacy.

2 Informatiebeveiligingsbeleid

2.1 Informatiebeveiliging

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader dat de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van gemeentelijke informatie(systemen) bevordert. Deze Baseline is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. Deze Baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2017 en NEN/ISO 27001:2017. 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, SUWI-wet, BRP, BAG en PUN.

Het informatiebeveiligingsbeleid is volgens de NEN/ISO 27000 normen op schrift gesteld. Onder informatiebeveiliging wordt in dit kader verstaan een samenhangend geheel van maatregelen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de informatiehuishouding en de controleerbaarheid van de getroffen maatregelen garandeert.

2.2 Raakvlakken met ander beleid

Het door het college vastgestelde strategisch informatiebeveiligingsbeleid en het door de directie vastgestelde technisch- en algemeen-informatiebeveiligingsbeleid zijn de kapstok voor het opstellen van dit informatiebeveiligingsplan BRP en waardedocumenten. Dit informatiebeveiligingsplan BRP en waardedocumenten is gericht op de specifieke maatregelen en inrichting van de betreffende wet- en regelgeving en vertaalt zich in specifieke procedures en werkwijzen. Meer informatie over de raakvlakken met ander soort beleid, procedures en rapportages is omschreven op pagina 17 hoofdstuk 4 ‘’Meer informatie.’’

2.3 Beleidsdoelstelling Oosterhout

Het gemeentebestuur van Oosterhout stelt zich ten aanzien van de informatiebeveiliging als doel om beveiligingsmaatregelen te treffen die de continuïteit van de dienstverlening aan inwoners en ondernemers en de bedrijfsvoering borgen. Maatregelen richten zich op de 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 Oosterhout de uiteindelijke verantwoordelijkheid draagt. Op het gebied van de BRP en waardedocumenten neemt zij daarbij de algemene en specifieke eisen vanuit wet en regelgeving als uitgangspunt. Er is een bedrijfscontinuïteitsplan aanwezig welke zorg draagt voor de continuïteit van alle gemeentelijke processen. Onderdeel daarvan is het continuïteitsplan Burgerzaken welke de continuïteit voor de processen binnen burgerzaken waarborgt in geval van een calamiteit.

Als concrete norm voor de realisering van de beleidsdoelstelling wordt de eis neergelegd dat de informatiesystemen aangeduid in dit plan een beschikbaarheid kennen van minimaal 99,0% tijdens kantoortijd.

2.4 Wettelijk kader verwerking persoonsgegevens

In de Algemene verordening gegevensbescherming (AVG) zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd. Dit betekent dat dezelfde privacywetgeving geldt in de hele Europese Unie.
De Wet BRP kent een eigen stelsel van regels. Op de verwerking van persoonsgegevens die in de BRP voorkomen, is de AVG niet van toepassing. De Autoriteit Persoonsgegevens houdt wel toezicht op de uitvoering van de Wet BRP (op grond van artikel 4.1 Wet BRP).

De Wet BRP vormt het algemeen kader voor de verwerking en het juiste gebruik van persoonsgegevens. Daarbij gaat het onder andere over hoe de gegevens juist worden opgenomen, gewijzigd en verstrekt. In de AVG staan een aantal aanvullende regels voor het verwerken van persoonsgegevens deze gaan over de situaties die in de Wet BRP niet zijn geregeld. De aanvullende regels zijn als volgt:

U heeft als verwerkingsverantwoordelijke voor de BRP onder meer de volgende plichten op grond van de AVG:

- De regels volgen bij het inschakelen van verwerkers (artikel 28 AVG);
- Een verwerkingsregister bijhouden (artikel 30 AVG);
- Datalekken melden (artikel 33 en 34 AVG);
- Een functionaris gegevensbescherming (FG) aanwijzen (artikel 37 en 38 AVG).

Zowel in de Wet BRP als in de AVG staat een kennisgevingsplicht:

- Artikel 3.23, eerste lid van de Wet BRP;
- Artikel 19 AVG;
- Artikel 23 AVG.

De kennisgevingsplicht houdt in dat de gemeente het aan andere organisaties moet laten weten wanneer zij persoonsgegevens in de BRP hebben gerectificeerd of gewist. Toch hoeft dit niet altijd te gebeuren. In artikel 19 van de AVG staat dat ontvangers niet geïnformeerd hoeven te worden als dit onmogelijk blijkt of onevenredig veel inspanning zou kosten.

In de praktijk krijgen bepaalde ontvangers al automatisch een seintje als er wijzigingen zijn in de persoonsgegevens die zij gewoonlijk ontvangen. Dat zijn ontvangers die bij ministerieel besluit zijn geautoriseerd voor spontane mutatieverstrekkingen uit de BRP.

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.

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

2.5 Taken, verantwoordelijkheden en bevoegdheden

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

De CISO is verantwoordelijk voor de strategische beleids- en planvorming en strategische en tactische advisering op het gebied van de informatievoorziening.

De beveiligingsbeheerder is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van dit informatiebeveiligingsplan en ziet erop toe dat eens per jaar gecontroleerd wordt of de nog te nemen maatregelen gerealiseerd zijn.

De beveiligingsfunctionaris is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van het informatiebeveiligingsplan voor de gemeentelijke voorzieningen waarmee de gemeente Oosterhout uitvoering geeft aan de Wet BRP.

2.5.1 Verantwoordelijkheden College B&W, directie en management

Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Oosterhout. Voor alle gegevensverwerkende processen rond het beheer en uitgifte van waardedocumenten heeft de burgemeester op basis van de Paspoortwet en het Regelement Rijbewijzen de uiteindelijke verantwoordelijkheid.

Genoemde bestuursorganen onderschrijven de beveiligingsmaatregelen die in dit informatiebeveiligingsplan 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.

Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van dit informatiebeveiligingsplan is de rol van de beveiligingsfunctionaris 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 dit plan en daarover aan het college van B&W respectievelijk de burgemeester te rapporteren.
De functie van de beveiligingsfunctionaris BRP/PNIK kent zeer specifieke taken en verantwoordelijkheden op het beveiligingsgebied van de wet BRP, reisdocumenten en de rijbewijzen.

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle leden van het managementteam van de gemeente Oosterhout. Voor BRP en waardedocumenten is de Teamleider Eerste Lijn & Burgerzaken verantwoordelijk voor het proces en bepaalt binnen de gegeven bestuurlijke kaders de richting van het ambtelijk apparaat.

De CISO en FG hebben een adviserende en ondersteunende rol. Taakbeschrijving van de CISO en FG zijn te vinden in het overkoepelend Informatiebeveiligingsbeleid.

2.6 Passende technische en organisatorische maatregelen

Welk niveau van technische en organisatorische maatregelen passend is, wordt bepaald door de risicoklasse waarin de persoonsgegevens worden ingedeeld en de context waarbinnen de gegevens worden verwerkt[2].
De in de BRP vastgelegde persoonsgegevens zijn op basis van het basisbeveiligingsniveau-principe (BBN) geclassificeerd met niveau 2+ (hoog op beschikbaarheid, integriteit en vertrouwelijkheid). Duidelijk hierbij is dat een betrokkene negatieve gevolgen ondervindt bij verlies (of niet beschikbaar zijn), niet correct (up-to-date) en inzichtelijk voor onbevoegden van deze persoonsgegevens.

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.

2.6.1 Kwaliteitsaspecten

Door middel van controles op de uitvoering dient het managementteam vast te stellen of de maatregelen werken. De beveiliging van gegevens kent vier kwaliteitsaspecten, namelijk:

1e: **beschikbaarheid**	De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.
2e: **integriteit**	De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
3e: **vertrouwelijkheid**	Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.
4e: **controleerbaarheid**	Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trail) van groot belang. Controleerbaarheid is de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd en gebruikt.

[2] Richtsnoeren beveiliging van persoonsgegevens, Cbp 2013

2.6.1.1 Norm voor beschikbaarheid

Gemeente Oosterhout hanteert voor deze kwaliteitsaspecten de volgende normen:

Het college van B&W en het managementteam zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening wordt gestaakt als gevolg waarvan een aantal bedrijf kritische applicaties niet meer kan 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 **99,0%**.
Het functioneren van de BRP is cruciaal tijdens de openingstijden voor het publiek.
Deze zijn: op maandag t/m donderdag van 8.30-17.00 uur, donderdagavond van 17.00-20.00 uur; vrijdag 08.30-12.00 uur.
Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt op jaarbasis tijdens kantooruren voor **99,0%** beschikbaar te zijn.
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 gemeentevoorzieningen treft die onverhoopte uitval van 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 gemeentelijke 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 hervatten.

2.6.1.2 Norm voor integriteit

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

Het is niet te voorkomen dat gegevens fouten bevatten. Een BRP-bestand zonder fouten is een nobel streven, maar 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	Norm zelfevaluatie 2023
1 (A)	99,70
2 (B)	99,70
3 (C)	99,60
4 (D)	99,50
5 (E)	99,50
6 (F)	99,40

Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens accepteert de gemeente per afzonderlijke klasse een score die minimaal gelijk is aan de score zoals die in bovenstaande tabel is opgenomen.

2.6.1.3 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 en op aangeven van de direct leidinggevende van de betreffende persoon. Degenen die inzage hebben in de BRP en/of belast zijn met de bijhouding van de BRP en/of werken met waardedocumenten dienen een geheimhoudingsverklaring te hebben ondertekend.

De medewerkers van team Eerste lijn en Burgerzaken moeten op de hoogte zijn van de bepalingen in de paspoortuitvoeringsregeling Nederland (PUN) en nauwkeurig volgens deze voorschriften werken. Daarnaast moeten zij allen op de hoogte zijn van de inhoud van het Informatiebeveiligingsplan BRP en waardedocumenten. Zij tekenen eens in het jaar een aftekenlijst voor gezien en gelezen van het Informatiebeveiligingsplan BRP en waardedocumenten.

Bevoegde medewerkers zijn allen in het bezit van een toegangspas welke toegang geeft tot het Reisdocumenten Aanvraag en Archiefstation (RAAS) en het Rijksdienst Wegverkeer (RDW) station. Het wachtwoord moet bij voorkeur eens in de drie maar uiterlijk eens in de zes maanden worden gewijzigd. De medewerkers tekenen een aftekenlijst wanneer het wachtwoord is gewijzigd.

2.6.1.4 Norm voor controleerbaarheid

Mutaties in persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente Oosterhout 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 Oosterhout 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 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 dit informatiebeveiligingsplan 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.

Als grondslag voor het beveiligingsbeleid op het onderdeel BRP 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 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(PUN). 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 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 zorgdragen 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 dit informatiebeveiligingsplan voorgestelde beveiligingsmaatregelen en –procedures vormen voor een groot deel eens per jaar het object van onderzoek bij de door de Paspoortwet en Wet BRP (artikel 4.3) voorgeschreven zelfevaluaties. De uitslagen van deze zelfevaluaties worden door respectievelijk de burgemeester en het college van B&W naar de Rijksdienst voor Identiteit gegevens (RvIG) gezonden en openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. De Kwaliteitsmonitor is er ook voor de controle op de inhoudelijke kwaliteit van de gegevens op de persoonslijsten in de basisregistratie personen (BRP) van de inwoners van Oosterhout.

3.2.2 Onderzoek BRP gegevens

De Rijksdienst voor Identiteit Gegevens (RvIG) voert maandelijks inhoudelijke kwaliteitscontroles uit. Dat gebeurt met de Bestandscontrolemodule (BCM). Deze applicatie controleert of de structuur van de persoonslijst klopt, of de ingevulde waarden toegestaan zijn en of de inhoud voldoet aan de voorschriften van het Logisch Ontwerp (LO).
De uitkomsten van de controles worden maandelijks via de webapplicatie Kwaliteitsmonitor aan gemeenten gerapporteerd. In overleg met alle Nederlandse gemeenten zijn normen vastgesteld over het percentage fouten in de basisregistratie. De gemeenten zetten de

uitkomsten van de controles van de maand december, afgezet tegen de vastgestelde normen, in de jaarlijkse rapportage van de zelfevaluatie.
Elke gemeente kan de resultaten van de op haar betrekking hebbende onderdelen van de BRP in het onderdeel **gegevens → uw gemeente** terugvinden in de Kwaliteitsmonitor bekijken met behulp van een persoonlijke login. De gegevens in de BRP moeten voldoen aan de kwaliteitsnormen.

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 digitale vragenlijsten BRP die de Rijksdienst voor Identiteit Gegevens (RvIG) via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt.

Informatieveiligheidsvragen zijn vragen die gaan over de inrichting en beveiliging van de systemen waarin de persoonsgegevens worden opgeslagen. De informatieveiligheidsvragen van de zelfevaluatie BRP worden door de gemeenten beantwoord via de tool van Eenduidige Normatiek Single Information Audit (ENSIA).

De vragenlijsten moeten jaarlijks **vóór 1 januari** definitief zijn ingevuld.

De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, mag aangevuld met een eventueel te nemen actieplan van de gemeente ter kennis worden gebracht aan het college van B&W. Indien deze akkoord zijn bevonden worden de ondergetekende rapportages **vóór 30 april** naar de RvIG en de Autoriteit Persoonsgegevens (AP) doorgezonden.

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

3.2.4 Onderzoek Paspoorten en NIK

Al enige tijd gebruiken gemeenten voor het onderzoek naar het reisdocumentenproces de vragenlijst in de Kwaliteitsmonitor van de RvIG. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks **vóór 1 januari** definitief zijn ingevuld. De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, mag aangevuld met de eigen bevindingen van de beveiligingsfunctionaris waardedocumenten en voorzien van een eventueel actieplan ter kennis worden gebracht aan de het college van B&W. Het bestuursorgaan, de burgemeester, ondertekent de rapportage waarna deze **vóór 30 april** naar de RvIG wordt doorgestuurd. De beveiligingsfunctionaris waardedocumenten neemt kennis van 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 geconstateerde tekortkomingen worden schriftelijk vastgelegd en de daarop betrekking hebbende rapportages worden vijf jaar bewaard. Op de eventueel geconstateerde tekortkomingen wordt actie ondernomen.

3.3 Taken, verantwoordelijkheden en bevoegdheden

Op grond van de Wet BRP, de Paspoortwet en het Reglement Rijbewijzen dient een aantal taken, verantwoordelijkheden en bevoegdheden te worden vastgelegd en belegd in de organisatie. Zolang de gemeente de Wet BRP uitvoert met de gemeentelijke voorzieningen die de AVG voorschrijft, dan betreft dit de beheerrollen die betrekking hebben op het informatiebeheer, gegevensbeheer, privacybeheer, applicatiebeheer en systeembeheer.

Op het gebied van de waardedocumenten dient een beveiligingsfunctionaris te worden aangewezen.

3.4 Functiescheiding Waardedocumenten

Om de kans te verkleinen dat medewerkers van het Team Eerste Lijn & Burgerzaken 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	Vaststellen identiteit en aannemen van de aanvraag.
Verstrekking	Beoordelen en controleren aanvraag en de aanvraag verzenden Naar de producent.
Beheer:	Controleren verwachte ontvangsten controleren document controleren personalisatie controleren openstaande aanvragen en systeemsignalen en het inklaren van de documenten.
Uitreiking:	Verifiëren identiteit, innemen en vernietigen oude documenten Uitreiken document

3.4.1 Functiescheiding Reisdocumenten

Voor de invoering van de functiescheiding gaat vanaf 1 januari 2025 de Paspoortuitvoeringsregeling Nederland (PUN) voorschrijven dat er altijd minimaal drie verschillende personen betrokken zijn bij de verschillende handelingen in de aanvraag en uitgifte van paspoorten en identiteitskaarten. Er is in het bijzonder aandacht voor de rol van verstrekker (de persoon die het verstrekking besluit neemt).

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

- Tussen de beveiligingsfunctionaris waardedocumenten en degenen die belast zijn met uitvoerende en beheertaken met betrekking tot reisdocumenten (PUN-artikel 93, lid 10).
- De beveiligingsfunctionaris waardedocumenten mag niet betrokken zijn bij of verantwoordelijkheid dragen voor de procedures rondom reisdocumenten. Dit voorkomt dat de beveiligingsfunctionaris waardedocumenten zijn eigen werk controleert.
- Tussen aanvraag/verstrekking, beheer en uitreiking van reisdocumenten (PUN-artikel 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 applicatie iBurgerzaken van Pink Roccade maakt het technisch onmogelijk om de aanvrager van het document ook het document te laten uitreiken in het systeem.
- 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 hiervoor de 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 waardedocumenten 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 functiescheiding te worden gerealiseerd tussen de aanvraag en de uitreiking van rijbewijzen. Het rijbewijs wordt door een andere medewerker uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

De applicatie iBurgerzaken van Pink Roccade maakt het technisch onmogelijk om de aanvrager van het document ook het document te laten uitreiken in het systeem.

Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Zie hiervoor de 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 waardedocumenten of de schriftelijke vastlegging aanwezig is en de aanvraag, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

4 Meer informatie

Beleidsstukken, procedures en rapportages hebben raakvlakken met dit informatiebeveiligingsplan. Onderstaand zijn ze allemaal onder elkaar gezet.

1. Algemeen

A. Raakvlakken met interne en externe bronnen en beleid

Intern:

- Verordening gegevensverstrekking /Reglement basisregistratie personen gemeente Oosterhout 2017
- Algemeen mandaat-, volmacht-, en machtigingsbesluit 2011 (geldend van 01-01-2015 t/m heden)
- Algemeen Beleid voor informatieveiligheid en privacybescherming gemeente Oosterhout 2024 inclusief de melding van incidenten
- Continuïteitsbeheer, Clear desk policy, autorisatie lokale netwerk Equalit
- Agressieprotocol gemeente Oosterhout
- Verwerkingsregisters en DPIA Privacy
- Autorisatie en geheimhouding verzoek tot raadplegen BRP in JIRA
- Toegangsbeveiliging en beleid SID

Extern:

- Trusted Platform Module (TPM) informatiebeveiliging SaaS applicatie voor de BRP van PinkRoccade
- Bijlage 3_modelwerkinstructie bij identiteitsfraude

B. Procedures

01. In en uit Dienst
02. Vernietiging van verwijderbare media + procedure van transport *****
03. Communicatie over beveiliging
04. Goedkeuren updates applicatie *****
05. Kasbeheer
06. Procedure Protocolleren (handleiding pinkroccade iBZ)

***ICT**

2. BRP

B. Procedures

01. Procedure autorisatie tot de BRP en GBA-V
02. Correctie
03. Gegevensverwerking
04. Identificatie en Machtiging
05. Inzagerecht
06. Protocollering
07. Terugmeldingen
08. Verstrekken van gegevens aan organen van de gemeente
09. Verstrekken van gegevens uit de BRP
10. Verstrekkingsbeperking

3. Waardedocumenten

B. Procedures

01. Aanvraag en uitreiking waardedocumenten
02. Autorisatie RAAS aanvraagstations en rijbewijsmodule
03. Ontbreken van voldoende functiescheiding
04. Ontvangst en beheer waardedocumenten
05. Procedure controleren van reisdocumentenadministratie
06. Procedure identificatie
07. Opname of vervallen reisdocument
08. Weigeren aanvraag reisdocument

C. Rapportages

01. Controle Autorisaties RAAS aanvraagstations en rijbewijsmodule
02. Controle ontbreken van voldoende functiescheiding
03. Rapportage controle communicatie over beveiliging
04. Evaluatie rijbewijzen
05. Pre-DPIA BIV classificatie iBurgerzaken 2024