GEMEENTEBLAD
Officiële uitgave van de gemeente Haarlemmermeer
Nr. 143578
12 juni
2019

Plan informatiebeveiliging Basisregistratie personen en waardedocumenten

Burgemeester en wethouders van de gemeente Haarlemmermeer,
gelet op de Wet Basisregistratie personen en de Algemene Verordening Gegevensbescherming,
besluiten:
Vast te stellen het navolgende Plan informatiebeveiliging Basisregistratie personen en waardedocumenten:

Hoofdstuk 1: Algemene basisbeginselen

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 voor de BRP zijn de burgemeester en het college van burgemeester en wethouders. 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 dient een plan aangaande informatiebeveiliging BRP en waardedocumenten ten grondslag te liggen. De uitgangspunten en beveiligingsprocedures, die invulling aan de gestelde eisen moeten geven, worden in dit plan opgenomen. Dit document is aanvullend op het Informatiebeveiligingsbeleid en het privacyreglement gemeente Haarlemmermeer 2018 en vormt de basis voor de uit te voeren (informatie) beveiligingsprocedures binnen de wet- en regelgeving van burgerzaken. Alle uitvoerende processen, rapportages en formulieren waarnaar wordt verwezen, worden jaarlijks geactualiseerd en vastgesteld door de teammanager burgerzaken.

1.2 Inleiding

De Gemeente Haarlemmermeer is 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 staat voorgeschreven, dat het treffen van beveiligingsmaatregelen noodzakelijk is. De gemeente verwerkt persoonsgegevens ook binnen tal van andere processen, waarbij evengoed wettelijke regels kunnen gelden. Ook buiten het domein van persoonsgegevens is er sprake van processen waarbij informatiebeveiliging noodzakelijk is, bijvoorbeeld tijdens besluitvormingsprocessen waarbij de Gemeente Haarlemmermeer als belanghebbende nadeel kan ondervinden van het te vroeg in de openbaarheid komen van genomen besluiten.

Een gemeentebreed beveiligingsbeleid, zoals vastgesteld in 2018, met daarop afgestemde plannen is noodzakelijk om de totale bedrijfsvoering van de Gemeente Haarlemmermeer te beveiligen. Dit plan informatiebeveiliging BRP en waardedocumenten staat op zichzelf, 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 IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en richt zich op bewustwording en concrete (incident)ondersteuning omtrent informatiebeveiliging.

1.3 Totstandkoming, implementatie en evaluatie

1.3.1 Permanent overleg in BAC

Ten behoeve van het gemeentelijke Informatiebeveiligingsbeleid heeft de gemeente Haarlemmermeer een permanente overlegstructuur; de Beveiligings Advies Commissie (BAC). Burgerzaken is , in het kader van informatiebeveiliging BRP en waardedocumenten, onderdeel van de BAC. De leden van de BAC vervullen een sleutelrol bij het beheer van de gemeentelijke voorzieningen, het beheer van waardedocumenten of bij de (fysieke) beveiliging van het gemeentehuis. De burgerzaken leden van de BAC vervullen deze rol onder de verantwoordelijkheid van de teammanager Burgerzaken, de coördinatie ligt in handen van de Beveiligingsbeheerder burgerzaken.

1.3.2 Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als dit op een gestructureerde manier wordt georganiseerd en de betrokken actoren de hun toegewezen taken op correcte wijze uitvoeren. Beleidsdoelstellingen zijn bepalend voor de invulling van het informatiebeveiligingsbeleid en in dit Informatiebeveiligingsplan 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 mede verantwoordelijk voor de uitvoering van het beleid. Op basis van hun rollen en taken binnen de organisatie worden verantwoordelijkheden aan hen toegewezen.

Het Informatiebeveiligingsplan burgerzaken wordt, in het kader van de jaarlijks terugkerende zelfevaluaties en het ENSIA proces, jaarlijks geëvalueerd door de beveiligingsbeheerder burgerzaken, in samenspraak met de chief information security officer (CISO). De beveiligingsbeheerder burgerzaken controleert of de in het plan opgenomen procedures nog steeds relevant en actueel zijn en stelt deze indien nodig bij. Alle medewerkers van burgerzaken worden via de gebruikelijke interne kanalen geïnformeerd over wijzigingen binnen het informatiebeveiligingsbeleid, het Informatiebeveiligingsplan 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.

Het plan Informatiebeveiliging BRP en waardedocumenten bevat een stelsel van procedures en maatregelen die bestemd zijn voor toepassing in de dagelijkse praktijk. De betreffende procedures op het gebied van BRP en waardedocumenten moeten periodiek worden bezien op actualiteit. In dit plan zijn daarom duidelijke afspraken vastgelegd omtrent de verantwoordelijkheid voor de handhaving en naleving van getroffen maatregelen en procedures.

Voorliggend document Informatiebeveiliging BRP en waardedocumenten wordt jaarlijks in het kader van de verplichte zelfevaluaties geëvalueerd en zo nodig geactualiseerd. Het gehele document dient minimaal eenmaal per raadsperiode te worden herijkt.

1.4 Verantwoording

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) vormt het normenkader waaraan de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van gemeentelijke informatie(systemen) dient te voldoen. De BIG is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat dat voor iedere gemeente geldt. De BIG 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 BIG ook gebruik gemaakt van onder andere de AVG, de SUWI-wet, BRP, Basisadministratie Adressen en gebouwen (BAG) en Paspoort uitvoeringsregeling Nederland 2001 en de Paspoortuitvoeringsregeling Buitenland 2001 (PUN).

Dit plan Informatiebeveiliging BRP en waardedocumenten is afgestemd op het Informatiebeveiligingsbeleid Haarlemmermeer 2018 en dat voldoet aan de inhoud van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van KING.

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

Hoofdstuk 2: Beleidsuitgangspunten informatiebeveiligingsbeleid

2.1 Informatiebeveiliging

Het geldende informatiebeveiligingsbeleid is opgesteld volgens de voorgeschreven NEN/ISO 27000 normen en vervolgens door het gemeentebestuur, de gemeentesecretaris en het directieteam 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.

2.2 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.

Het informatiebeveiligingsbeleid BRP en waardedocumenten heeft werking binnen burgerzaken en is aanvullend op het informatiebeveiligingsbeleid van de gemeente, zoals beschreven in de (bijlagen van de) nota privacy, informatiebeveiliging en informatiebeheer 2018. Dit plan Informatiebeveiliging BRP

en waardedocumenten is gebaseerd op de inhoud van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

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 'clear desk beleid' (ook wel 'clean desk policy' genoemd).

2.3 Beleidsdoelstelling

Het gemeentebestuur van de Gemeente Haarlemmermeer neemt zich ten aanzien van de informatiebeveiliging voor, om beveiligingsmaatregelen te treffen die de continuïteit van de bedrijfsvoering garanderen. De verschillende soorten maatregelen richten zich in ieder geval op beschikbaarheid, integriteit, vertrouwelijkheid van gegevens en de controleerbaarheid van de gemeentelijke bedrijfsprocessen. Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het gemeentebestuur van de Gemeente Haarlemmermeer de uiteindelijke verantwoordelijkheid draagt. Op het gebied van de BRP en waardedocumenten neemt zij daarbij het wettelijk kader als uitgangspunt.

Als concrete norm voor de realisering van de beleidsdoelstellingen wordt de eis gehanteerd dat de informatiesystemen zoals aangeduid in dit plan, tijdens de werktijden van burgerzaken (inclusief gemeentebalie Schiphol) voldoen aan de beschikbaarheidseis van minimaal 99,9%. Buiten de werktijden worden er geen eisen gesteld aan de beschikbaarheid van de systemen met uitzondering van voorzieningen die in het kader van rampenbestrijding zijn getroffen.

2.4 Wettelijk kader verwerking persoonsgegevens

De Algemene Verordening Gegevensbescherming (AVG) vormt het algemeen kader voor de verwerking en beveiliging van persoonsgegevens.

De Nederlandse toezichthouder van de AVG, 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 dit plan zijn: de Wet BRP, de Paspoortwet en het Reglement rijbewijzen. Relevant voor dit plan is dat de AVG voor 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 het plan Informatiebeveiliging BRP en waardedocumenten ligt bij het college van B en W respectievelijk de burgemeester. Deze organen zien toe op de opstelling en uitvoering daarvan.

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

De beveiligingsbeheerder burgerzaken is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van dit plan Informatiebeveiliging BRP en waardedocumenten waarmee de Gemeente Haarlemmermeer uitvoering geeft aan de Wet BRP en het gegevensmagazijn.

De CISO is in samenwerking met de beveiligingsbeheerder burgerzaken verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van het plan 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, waarin de taken, verantwoordelijkheden en benoemingen van functionarissen binnen burgerzaken geregeld wordt).

2.5.1 Verantwoordelijkheden gemeentebestuur
Beveiliging op bestuurlijk niveau betreft de verantwoordelijkheid van het college van B en W van de Gemeente Haarlemmermeer. Het college van B en W stelt het deel over Informatiebeveiliging BRP vast en de burgemeester stelt het onderdeel waardedocumenten vast.

Voor alle gegevensverwerkende processen rondom het beheer en de uitgifte van waardedocumenten draagt de burgemeester op basis van de Paspoortwet en het Reglement rijbewijzen de uiteindelijke verantwoordelijkheid.

Genoemde bestuursorganen onderschrijven de beveiligingsmaatregelen die in dit plan Informatiebeveiliging BRP en waardedocumenten worden voorgeschreven volledig en besluiten, 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 het plan Informatiebeveiliging BRP en waardedocumenten is de samenwerking van de CISO en de beveiligingsbeheerder burgerzaken van belang. Deze hebben gezamenlijk de verantwoordelijkheid om namens de bestuursorganen toe te zien op naleving van de beveiligingsmaatregelen en -procedures zoals uitgewerkt in het plan Informatiebeveiliging BRP en waardedocumenten en daarover aan het college van B en W respectievelijk de burgemeester te rapporteren.

De functie van 'de beveiligingsbeheerder' binnen burgerzaken moet niet verward worden met de functie van 'de beveiligingsfunctionaris reisdocumenten en rijbewijzen'. Beide functies kennen zeer specifieke taken en verantwoordelijkheden op het gebied van enerzijds de beveiliging van reisdocumenten en anderzijds de beveiliging van rijbewijzen. De grondslag hiervoor ligt in de Paspoortuitvoeringsregeling (PUN)[1]

2.5.2 Verantwoordelijkheden van de clustermanagers
Beveiliging op ambtelijk niveau, betreft de verantwoordelijkheid van alle clustermanagers van de Gemeente Haarlemmermeer.

De directie bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

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

1. De voortgang van de realisatie van beveiligingsmaatregelen zoals beschreven in het plan Informatiebeveiliging BRP en waardedocumenten, gerapporteerd door de beveiligingsbeheerder (zo nodig in samenspraak met de CISO)
2. Het benoemen van mogelijke ontwikkelingen die de bedrijfsinformatie kunnen bedreigen.
3. Het toezicht op en de bespreking van beveiligingsincidenten, zoals gerapporteerd door de beveiligingsfunctionaris reisdocumenten of de beveiligingsfunctionaris rijbewijzen.
4. Beoordeling en Goedkeuring van initiatieven om de (informatie)beveiliging te verbeteren.
5. Het geven van zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen.
6. Het bevorderen van het beveiligingsbewustzijn.
7. De noodzaak tot herziening en goedkeuring van het beveiligingsbeleid en de toegekende verantwoordelijkheden.

2.5.3 Verantwoordelijkheden van de chief information security officer (CISO)
De CISO is op gemeentelijk niveau verantwoordelijk voor de informatiebeveiliging. De CISO geeft functioneel leiding aan het werk van de beveiligingsbeheerders op de lagere niveaus. 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 directieteam op waarde moeten kunnen beoordeeld.

De CISO is verantwoordelijk voor:
1. het opstellen van het gemeentebrede plan Informatiebeveiliging;
2. de voortgang en de realisatie van beveiligingsmaatregelen zoals beschreven in het plan Informatiebeveiliging;
3. het actualiseren van het gemeentebreed Informatiebeveiligingsplan;
4. het gezamenlijk met beveiligingsbeheerders afstemmen van de maatregelen op afdelingsniveau, waaronder met de beveiligingsfunctionaris reisdocumenten en rijbewijzen.

Tevens dient de CISO:
1. rechtstreeks te rapporteren aan de directeur bedrijfsvoering;

2. gevraagd en ongevraagd de informatiebeveiliging van de Gemeente Haarlemmermeer te bevorderen.
3. de rapportages, zoals die vanuit ENSIA verplicht zijn, 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 Haarlemmermeer.

2.5.4 Verantwoordelijkheden van overige rollen/functies
De verantwoordelijkheden van de rollen en/of functies van de informatiebeheerder, gegevensbeheerder, privacybeheerder burgerzaken, applicatiebeheerder, toezichthouder BRP, fraude coördinator, systeembeheerder en beveiligingsbeheerder burgerzaken zijn vastgelegd in de door het college vastgestelde Regeling beheer en Toezicht BRP.

Voor alle in dit plan informatiebeveiliging BRP en waardedocumenten voorkomende functies moet de benoeming en vervanging worden vastgelegd.

2.5.5 Passende technische en organisatorische maatregelen
Welk niveau van technische en organisatorische maatregelen passend is, wordt bepaald door de risicoklasse waarin de persoonsgegevens worden ingedeeld en de context waarbinnen de gegevens worden verwerkt.

De in de BRP vastgelegde persoonsgegevens zijn op grond van de door de AP gehanteerde classificatie ingedeeld in risicoklasse II (verhoogd risico). Dat wil zeggen dat er in vergelijking met het basisniveau van risicoklasse I extra negatieve gevolgen bestaan 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 Haarlemmermeer.

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:

1. risico's van de verwerking, op basis van de aard van de persoonsgegevens en de omvang van verwerking;
2. de stand van de techniek;
3. de kosten van de te treffen maatregelen.

2.5.6 Kwaliteitsaspecten
Het Informatiebeveiligingsbeleid 2018 omvat de verantwoordelijkheden en werkwijze waarmee Gemeente Haarlemmermeer dient te komen tot adequate informatiebeveiliging. De nota en het informatiebeveiligingsbeleid vormen daarmee de basis voor de hieronder uitgewerkte normen en maatregelen en door dit plan kan verdere invulling gegeven worden.

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 vastgesteld te worden 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 beheersmaatregelen 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 zijn gestructureerd en gebruikt.

De gemeente Haarlemmermeer hanteert voor deze kwaliteitsaspecten de volgende normen:

2.6 Norm voor beschikbaarheid

Het college van B en W, het directieteam en het MT 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 99,9%. Het functioneren van de BRP is cruciaal tijdens de openingstijden voor het publiek. Het systeem dat de informatievoorziening BRP ondersteunt tijdens openingstijden dient een jaarlijks gemiddelde van 99,9% te handhaven.

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 BRP wordt uitgevoerd met behulp van de lokale voorzieningen die gebaseerd zijn op de Wet BRP (voorheen 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.

2.7 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 en de daarbij te hanteren instrumenten, zijn kwaliteitsindicatoren opgesteld voor de gegevens die in de BRP zijn opgenomen. Deze indicatoren zijn gebaseerd op het Logisch Ontwerp GBA[2] en op geldende regelgeving.

Aan de hand van kwaliteitsindicatoren wordt bepaald in hoeverre de vastgelegde gegevens in de BRP voldoen aan de vastgestelde eisen van de registratie.

Bij de uitgangspunten voor de beoordeling van de kwaliteitsindicatoren wordt onderscheid gemaakt tussen zes landelijk gehanteerde klassen:

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

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

2.8 Norm voor vertrouwelijkheid

Uitsluitend bevoegde personen in dienst van of werkzaam in opdracht van de Gemeente Haarlemmermeer hebben toegang tot en kunnen bij de uitvoer van hun taken, gebruik maken van de in de voor hen relevante registratie 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. Iedereen die belast is met de registratie van BRP-gegevens of werkt met waardedocumenten, dient een geheimhoudingsverklaring te hebben ondertekend.

2.9 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 Haarlemmermeer kent als norm, gebaseerd op het LO GBA, 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%.

2.10 Samenvatting

Beveiliging van (persoons-)gegevens vraagt om een zorgvuldige analyse van de risico's die met gegevensverwerking samenhangen. Er zijn verschillende risico's te noemen die ertoe kunnen leiden dat bedrijfsprocessen stagneren. 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 bijvoorbeeld onbetrouwbaar. De in dit plan Informatiebeveiliging BRP en waardedocumenten opgenomen procedures hebben als doel te voorkomen, dat de (kans op) risico's uit de aan verwerking van persoonsgegevens verbonden risicoklasse (II) zich voordoen. Uitvoering van deze procedures maakt het bedrijfsproces controleerbaar.

[1] Waarin dit document de PUN staat genoemd, wordt zowel de Paspoortuitvoeringsregeling Nederland 2001 (voor ingezetenen) als de Paspoortuitvoeringsregeling Buitenland 2001 (voor niet-ingezetenen) bedoeld.

[2] Logisch Ontwerp GBA versie 3.11 dan wel later vastgestelde versie.

Hoofdstuk 3: BRP en waardedocumenten

3.1 Wettelijk kader

3.1.1 Wet basisregistratie personen (Wet BRP)

Het op schrift stellen van de - in de praktijk van alledag al ingeburgerde - beveiligings procedures is noodzakelijk om objectief te kunnen bepalen of de BRP-bestanden en 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. De AVG is namelijk niet van toepassing op de gegevensverwerking in het kader van de BRP, omdat de Wet BRP en het Besluit BRP gaan vérder in het stellen van eisen aan de beveiliging dan de AVG.

Wel zijn een aantal bepalingen uit de UAVG van overeenkomstige toepassing verklaard in artikel 4.1 van de Wet BRP. Deze bepalingen betreffen de taken en bevoegdheden van de AP en het toezicht door de AP op de uitvoering van de Wet BRP.

Als grondslag voor het beveiligingsbeleid op het onderdeel BRP in dit plan zijn van belang de artikelen 1.10 en 1.11 van de Wet BRP. Artikel 1.10 bepaalt dat de beveiligingsmaatregelen BRP bij of krachtens Algemene Maatregel van Bestuur (AMvB) worden geregeld. Artikel 1.11 draagt het college van B&W op zich aan die maatregelen te houden.

Gelet op het belang voor het informatiebeveiligingsbeleid volgt hieronder de tekst van artikel 6 Besluit BRP. Bovendien geldt op grond van artikel 4.3 Wet BRP de verplichting om jaarlijks zelfonderzoek 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:*
    1. *maatregelen gericht op personen die werkzaam zijn voor de verantwoordelijke voor de verwerking van gegevens in de basisregistratie;*
    2. *maatregelen gericht op de toegang tot gebouwen en ruimten waar in de basisregistratie opgenomen gegevens aanwezig zijn;*
    3. *maatregelen gericht op een deugdelijke werking en beveiliging van de apparatuur en programmatuur;*
    4. *maatregelen voor het geval de geheimhouding of integriteit van in de basisregistratie opgenomen gegevens is geschaad;*
    5. *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 en de paspoortuitvoeringsregeling Buitenland 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 aan de hand van dit plan Informatiebeveiliging BRP en waardedocumenten verder uitgewerkt in concrete voorschriften op het gebied van fysieke beveiliging, back-up en herstel en enkele voorschriften over hoe te handelen in bepaalde situaties. Artikel 93 lid 1 PUN vereist daartoe organisatorische maatregelen.

3.1.3 Rijbewijzen
Het uitgifteproces van rijbewijzen komt sinds enkele jaren sterk overeen met dat van 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, ENSIA, onderzoek en accountantscontrole

3.2.1 Zelfevaluatie en ENSIA
De in het plan Informatiebeveiliging BRP en waardedocumenten voorgestelde beveiligingsmaatregelen en -procedures vormen eens per jaar het object van onderzoek, bij de door ENSIA, de Paspoortwet en Wet BRP voorgeschreven zelfevaluaties. Dit omvat de zelfevaluatie Paspoort en NIK, de zelfevaluatie Paspoort en NIK niet-ingezetenen, de zelfevaluatie BRP en de inhoudelijke controle op de kwaliteit van de BRP.

De uitslagen van deze zelfevaluaties worden door het college van B&W voor de BRP en door de burgemeester voor reisdocumenten, naar de Rijksdienst voor Identiteitsgegevens (RvIG) gezonden en openbaar gemaakt door de RvIG via de webapplicatie Kwaliteitsmonitor. De Kwaliteitsmonitor is ook de aangewezen applicatie voor de controle op de inhoudelijke kwaliteit van de gegevens in de BRP.

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 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.

3.2.3 Onderzoek BRP-processen
Gemeenten moeten periodiek zelf onderzoeken of zij voldoen aan de eisen die de wetgever stelt op het gebied van beveiliging en privacy bij de uitvoering van de BRP-werkzaamheden. Deze controle voert de gemeente uit aan de hand van een digitale vragenlijst BRP die de Rijksdienst voor Identiteitsgegevens via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt. De vragenlijst moet jaarlijks voor een bepaalde datum zijn ingevuld. De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beheerders en functionarissen van burgerzaken en voorzien van een actieplan van de gemeente) ter kennisgeving aan het college van B en W worden gestuurd voor ondertekening. De rapportage wordt vóór de daarvoor vastgestelde datum aan de Rijksdienst voor Identiteitsgegevens toestuurt.

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

3.2.4 Onderzoek paspoorten, NIK en rijbewijzen
Sinds april 2013 gebruiken gemeenten voor haar onderzoek naar het reisdocumentenproces de vragenlijst uit de Kwaliteitsmonitor. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks de daarvoor vastgestelde datum 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 deze wordt vóór de daarvoor vastgestelde datum naar de Rijksdienst voor Identiteitsgegevens gestuurd.

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

Ook de procedures rond het verstrekken van rijbewijzen zijn onderwerp van controle en worden op dezelfde manier geëvalueerd als de reisdocumenten. Gelijktijdig met de overige jaarlijkse zelfevaluaties.

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.

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 te worden belegd. Dit betreft de beheerrollen die betrekking hebben op de informatiebeheerder, de gegevensbeheerder, de beveiligingsbeheerder burgerzaken, de privacybeheerder burgerzaken, de toezichthouder BRP, de fraude coördinator, de applicatiebeheerder en de systeembeheerder.

Op het gebied van de waardedocumenten dienen te worden aangewezen een beveiligingsfunctionaris reisdocumenten, de autorisatiebevoegde reisdocumenten, de beveiligingsfunctionaris rijbewijzen en de autorisatiebevoegde rijbewijzen.

De toekenning van de rollen in het kader van de waardedocumenten worden na benoeming een bijlage van dit plan. Voor alle benoemde functies wordt vervanging vastgelegd.

3.3.1 Functiescheiding waardedocumenten
Om de kans te verkleinen dat medewerkers van de publieksbalie 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.

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

1. Tussen de beveiligingsfunctionaris reisdocumenten en degenen die belast zijn met uitvoerende- en beheertaken met betrekking tot reisdocumenten (PUN art. 93, lid 10).

2. 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.
3. 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.

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. Dit wordt jaarlijks gecontroleerd en vastgelegd.

Na afloop van de betreffende periode met te geringe capaciteit 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.

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

1. 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.

Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Dit wordt jaarlijks gecontroleerd en vastgelegd.

Na afloop van de betreffende periode controleert de beveiligingsfunctionaris rijbewijzen of de schriftelijke vastlegging aanwezig is en de aanvraag, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

Aldus besloten in de vergadering van het college van burgemeester en wethouders van 21 mei 2019.
Burgemeester en wethouders van Haarlemmermeer,

de secretaris, Drs. Carel Brugman
de burgemeester, Onno Hoes