gemeente lingewaard

GEMEENTEBLAD

Officiële uitgave van de gemeente Lingewaard

Nr. 144060

3 april 2023

Informatiebeveiligingsplan BRP met de regeling beheer en toezicht

Op 21 maart 2023 heeft het college vastgesteld het Informatiebeveiligingsplan BRP met de regeling beheer en toezicht 2023.

1 Algemeen

1.1 Algemeen

De wetgever stelt in de Wet basisregistratie personen (BRP), de Paspoortwet en het Reglement Rijbewijzen eisen aan de beveiliging van de uitvoeringsprocessen voor de BRP en Waardedocumenten. De verantwoordelijke bestuursorganen, burgemeester en wethouders voor de BRP respectievelijk de burgemeester[1] voor de andere twee processen, moeten jaarlijks rapporteren in hoeverre de organisatie aan deze eisen voldoet. Aan de beveiliging dient een Informatiebeveiligingsplan ten grondslag te liggen, waarin de uitgangspunten en beveiligingsprocedures zijn opgenomen die invulling geven aan die eisen. Dit document maakt deel uit van het in de vorige zin bedoelde Informatiebeveiligingsplan en vormt de basis voor de uit te voeren procedures met bijbehorende formulieren en rapportages waarnaar wordt verwezen in het hoofdstuk bijlagen.

1.2 Inleiding

BRP en Waardedocumenten zijn niet de enige bedrijfsprocessen waarvoor beveiliging noodzakelijk is en in de voornoemde wetten is voorgeschreven. De gemeente verwerkt op tal van plaatsen in de organisatie gegevens over personen, waarvoor de Wet AVG in artikel 32 de gemeente Lingewaard verplicht tot het treffen van beveiligingsmaatregelen. Ook buiten het domein van de persoonsgegevens valt er nog heel wat te beveiligen. Bijvoorbeeld besluitvormingsprocessen waarbij de gemeente Lingewaard als belanghebbende nadeel kan ondervinden als het besluit te vroeg in de openbaarheid komt.

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

De Wet basisregistratie personen (Wet BRP) is grondslag voor de basisregistratie van persoonsgegevens en vervangt de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA).

1.3 Totstandkoming, implementatie en evaluatie

1.3.1 overleggroep informatiebeveiliging BRP

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

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

1.3.2 Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt en alle factoren die daarbij een rol hebben, daar op een juiste manier invulling aan geven. Beleidsdoelstellingen zijn bepalend voor het informatiebeveiligingsbeleid en in dit plan zijn die specifiek gericht op het gebied van BRP en Waardedocumenten. Binnen de organisatie moeten medewerkers verantwoordelijkheden krijgen voor de implementatie van dit beleid.

De medewerkers worden betrokken (o.a. tijdens werkoverleg) bij de ontwikkeling en implementatie van het beleid en zijn mede verantwoordelijk voor de uitvoering. Daarnaast moet door de controller informatiebeveiliging worden vastgesteld of de maatregelen worden nageleefd.

Dit plan wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de beveiligingsbeheerder en bij noodzaak daartoe bijgesteld. Alle medewerkers van de gemeente Lingewaard worden via de gebruikelijke interne kanalen en voor zover noodzakelijk door hun leidinggevende via het regu-

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.

liere werkoverleg geïnformeerd over voor hen van belang zijnde wijzigingen in informatiebeveiligingsbeleid, -plan, -maatregelen en/of –procedures.

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

Dit plan Informatiebeveiliging BRP en Waardedocumenten bevat tevens een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden bezien op actualiteit. In dit plan zijn daarom afspraken vastgelegd over de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen en procedures met betrekking tot BRP en Waardedocumenten.

De belangrijkste afspraak in dit verband is dat overleggroep informatiebeveiliging BRP het voorliggend plan Informatiebeveiliging BRP en Waardedocumenten en de daarbij behorende procedures en bijlagen jaarlijks opnieuw bekijkt op actualiteit en controleert op naleving van de beleidsuitgangspunten.

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

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

1.4 Verantwoording
De Baseline Informatiebeveiliging Gemeenten (BIG) 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 27002:2007 en NEN/ISO 27001:2005. Deze standaard is voor de Nederlandse Overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Voor specifieke maatregelen is in onderhavige Baseline ook gebruik gemaakt van onder andere de WBP, SUWI-wet, BRP, BAG en PUN.

Dit plan Informatiebeveiliging BRP en Waardedocumenten is afgestemd met de inhoud van de Baseline Informatiebeveiliging Nederlandse gemeenten voor 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.

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

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

2 Informatiebeveiligingsbeleid
2.1 Informatiebeveiliging
Informatiebeveiligingsbeleid is volgens de NEN/ISO 27000 normen op schrift gesteld en door het gemeentebestuur, gemeentesecretaris en het managementteam goedgekeurde beveiligingsbeleid met betrekking tot de informatievoorziening.

Onder informatiebeveiliging wordt in dit kader verstaan een samenhangend geheel van maatregelen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens garandeert en de controleerbaarheid van de getroffen maatregelen.

2.2 Raakvlakken met ander beleid
Het informatiebeveiligingsbeleid heeft raakvlakken met het beleid en de daaruit voortvloeiende procedures die zijn gericht op de operationele veiligheid van het uitgifte- en beheerproces van waardedocumenten.

Informatiebeveiligingsbeleid maakt deel uit van het totale beveiligingsbeleid van de gemeente. Dit is beschreven in het gemeentebrede informatiebeleidsplan. Dit beleid is gebaseerd op de inhoud van de Baseline Informatiebeveiliging Nederlandse gemeenten voor Nederlandse Gemeenten (BIG).

Binnen dit beleidsterrein kan er onderscheid worden gemaakt tussen fysieke, logische en organisatorische beveiligingsmaatregelen met als voorbeelden identificatie van gebruikers, sleutelbeleid, personeelsbeleid en een clear desk policy.

2.3 Beleidsdoelstelling Lingewaard
Het gemeentebestuur van Lingewaard stelt zich ten aanzien van de informatiebeveiliging als doel om beveiligingsmaatregelen te treffen die de continuïteit van de bedrijfsvoering garanderen. Maatregelen kunnen bestaan uit fysieke, organisatorische en logische maatregelen. De verschillende soorten van maatregelen richten zich in ieder geval op beschikbaarheid, integriteit, vertrouwelijkheid van gegevens en de controleerbaarheid van de gemeentelijke bedrijfsprocessen. Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het gemeentebestuur van Lingewaard de uiteindelijke verantwoordelijkheid draagt. Op het gebied van de BRP en Waardedocumenten neemt zij daarbij de algemene en specifieke eisen van het wettelijk kader als uitgangspunt.

Als concrete norm voor de realisering van de beleidsdoelstelling wordt de eis neergelegd dat de informatiesystemen aangeduid in dit plan een beschikbaarheid tijdens werktijd kennen van minimaal 98%. Buiten werktijd worden er geen eisen gesteld aan de beschikbaarheid met uitzondering van voorzieningen in het kader van rampenbestrijding.

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

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

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

De kwaliteitsbeheerder BRP is in het bijzonder verantwoordelijk voor de opstelling, actualisering en uitvoering van het plan Informatiebeveiliging voor de gemeentelijke voorzieningen waarmee de gemeente Lingewaard uitvoering geeft aan de Wet BRP.

Beveiligingsfunctionaris reisdocumenten en overleggroep Informatiebeveiliging BRP en waardedocumenten is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van het 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).

2.5.1 Verantwoordelijkheden gemeentebestuur
Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Lingewaard. Het college van B&W stelt dit plan Informatiebeveiliging BRP vast en de burgemeester het onderdeel Waardedocumenten vast.

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

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

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

2.5.2 Verantwoordelijkheden Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) is op gemeentelijk niveau verantwoordelijk voor de informatiebeveiliging. De CISO geeft functioneel leiding aan het werk van de IB-functies op lagere niveaus. De CISO 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 moet kunnen beoordeeld.

De CISO is verantwoordelijk voor:

- Opstellen gemeentebreed plan Informatiebeveiliging;
- Voortgang en realisatie beveiligingsmaatregelen zoals beschreven in het plan Informatiebeveiliging;
- Actualiseren gemeentebreed informatiebeveiligingsplan;
- Afstemming met beveiligingsbeheerders op afdelingsniveau, waaronder de beveiligingsbeheerderen de beveiligingsfunctionaris Reisdocumenten en rijbewijzen.

De CISO rapporteert rechtstreeks aan de burgermeester.

De CISO bevordert en adviseert gevraagd en ongevraagd over de informatiebeveiliging van de gemeente Lingewaard. Ook verzorgt de CISO de rapportages over de status en kijkt of de genomen maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente Lingewaard.

2.5.3 Verantwoordelijkheden van overige rollen / functies

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

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

2.6 Passende technische en organisatorische maatregelen

Dit is reeds opgenomen in het informatiebeveiligingsbeleid van de gemeente Lingewaard.
De gemeente Lingewaard hanteert voor deze kwaliteitsaspecten de volgende normen:

2.6.1 Kwaliteitsaspecten

Informatiebeveiligingsbeleid omvat een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijke top eendrachtig duidelijk maken aan het tactisch en operationeel niveau welke gedragslijn de gemeente Lingewaard dient te volgen om te komen tot een adequate informatiebeveiliging. Het beleid vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Het maken en vaststellen van beveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten in een informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het 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:

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.

De gemeente Lingewaard hanteert voor deze kwaliteitsaspecten de volgende normen:

2.6.1.1 Norm voor beschikbaarheid

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 bedrijfs-

kritische applicaties niet meer kunnen functioneren. Dit geldt onder andere en in het bijzonder voor de informatievoorziening vanuit de BRP.
De informatievoorziening met betrekking tot de BRP moet tijdens de openingstijden van het gemeentehuis permanent beschikbaar zijn. In cijfers uitgedrukt betekent dit op jaarbasis een beschikbaarheid van gemiddeld 98%.

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

Maandag van 08:30 uur t/m 20:00 uur

Dinsdag t/m vrijdag van 08:30 uur t/m 17:00 uur

Daarnaast dient het systeem dat de informatievoorziening BRP ondersteunt op jaarbasis tijdens kantooruren voor 99% beschikbaar te zijn.

Met kantooruren worden hier bedoeld: 07:00 - 22:00 uur.

Aangezien de BRP in beheer is bij de landelijke overheid, is de gemeente voor de realisatie van deze norm afhankelijk van de landelijk beheerder. Voor de continuïteit in de bedrijfsvoering is het noodzakelijk dat de gemeente voorzieningen treft die onverhoopte uitval van het landelijke systeem kan opvangen. Dit betreft voorzieningen die betrekking hebben op de gegevensbestanden, netwerkverbindingen en lokale systemen.

De 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.

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 groepen van belang:

Tabel 2: Behaald percentage per klasse/groep

Groep (art 21 Reg.BRP)	Klasse	Omschrijving	Behaald percentage	Norm
1	A	Persoon en overlijden	99,98%	99.70%
	B	Adres	100,00%	99.70%
	C	Relaties	99,94%	99.60%
2	D	Identificatienummers en nationaliteit	99.98%	99.50%
	E	Overig algemeen	99.99%	99.50%
3	F	Administratief	99.98%	99.40%

Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens accepteert de gemeente Lingewaard een foutenpercentage zoals deze vermeld is in de kwaliteitsmonitor.
Daarnaast is het van belang dat de gegevens die over iemand zijn opgenomen in de BRP overeenkomen met de werkelijkheid. Om die reden wordt er fors geïnvesteerd in de voorkoming van dergelijke fouten,

bijvoorbeeld door adrescontroles uit te voeren, versterking van de samenwerking met ketenpartners en door actief in te zetten op preventie en bestrijding van fraude.

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

2.6.1.4 Norm voor controleerbaarheid

Mutaties in persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente Lingewaard 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 Lingewaard kent als norm dat 99% van alle mutaties in persoonsgegevens herleidbaar moeten zijn tot de individuele persoon die voor de mutatieverwerking verantwoordelijk was en dat zulks geldt voor 90% van alle raadplegingen.

Samenvatting

Beveiliging van (persoons-)gegevens vraagt om een zorgvuldige analyse van de risico's die met de gegevensverwerking samenhangen. Er zijn verschillende risico's te noemen die ertoe kunnen leiden dat bedrijfsprocessen stagneren. Bijvoorbeeld verlies van gegevens (raakt aan de kwaliteitsaspecten integriteit en beschikbaarheid) en onrechtmatig gebruik van gegevens (raakt aan het aspect vertrouwelijkheid), maken de resultaten van bedrijfsprocessen onbetrouwbaar. De in het voorliggend plan Informatiebeveiliging BRP en Waardedocumenten opgenomen procedures hebben als doel te voorkomen dat de risico's, behorend bij de aan de verwerking van persoonsgegevens verbonden risicoklasse (II) zich voordoen. Uitvoering van de procedures maakt het bedrijfsproces controleerbaar uit oogpunt van beveiliging.

3 BRP en Waardedocumenten

3.1 Wettelijk kader

3.1.1 BRP

Het op schrift stellen van de -in de praktijk van alledag al ingeburgerde- beveiligingsprocedures is noodzakelijk om objectief te kunnen bepalen of de BRP-bestanden en bepaalde processen voldoen aan de eisen ten aanzien van beschikbaarheid (continuïteit), integriteit (betrouwbaarheid), vertrouwelijkheid (exclusiviteit) en controleerbaarheid.
De gemeente moet op grond van de Wet BRP de beveiligingsmaatregelen nemen die de wet voorschrijft. Dit houdt in dat de volgende beveiligingsmaatregelen van toepassing zijn (artikel 32 AVG en artikel 6 Besluit BRP):

Artikel 32 Algemene Verordening Gegevensbescherming (AVG): Beveiliging van de verwerking

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

a) de pseudonimisering en versleuteling van persoonsgegevens;

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

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

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

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

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

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

Artikel 6 Besluit BRP

1. Het college van burgemeester en wethouders treft ten aanzien van de gemeentelijke voorziening passende technische en organisatorische maatregelen ter beveiliging van de in de basisregistratie opgenomen gegevens tegen verlies of aantasting van deze gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking van deze gegevens.
2. Onze Minister treft ten aanzien van de centrale voorzieningen passende technische en organisatorische maatregelen ter beveiliging van de in de basisregistratie opgenomen gegevens tegen verlies of aantasting van deze gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking van deze gegevens.
3. De in het eerste en tweede lid bedoelde maatregelen omvatten ten minste:
   a) maatregelen gericht op personen die werkzaam zijn voor de verantwoordelijke voor de verwerking van gegevens in de basisregistratie;
   b) maatregelen gericht op de toegang tot gebouwen en ruimten waar in de basisregistratie opgenomen gegevens aanwezig zijn;
   c) maatregelen gericht op een deugdelijke werking en beveiliging van de apparatuur en programmatuur;
   d) maatregelen voor het geval de geheimhouding of integriteit van in de basisregistratie opgenomen gegevens is geschaad;
   e) maatregelen bij calamiteiten.
4. Onze Minister kan regels stellen omtrent de bewaring van geschriften en andere bescheiden, ongeacht hun vorm, die de verantwoordelijke voor de verwerking van gegevens in de basisregistratie gebruikt of heeft gebruikt in verband met de verwerking van gegevens in de basisregistratie.

Bovendien geldt op grond van artikel 4.3 wet BRP de verplichting om jaarlijks uiterlijk op 31 december zelf onderzoek te doen naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie.

3.1.2 Reisdocumenten

De wetgever stelt eisen aan de opslag, uitgifte en administratie van reisdocumenten. Deze eisen zijn neergelegd in de Paspoortuitvoeringsregeling Nederland 2001, kortweg 'PUN' genoemd. Hoofdstuk XII van deze Regeling met als onderwerp beveiliging bepaalt in artikel 90: "De met de uitvoering van de wet belaste autoriteiten treffen maatregelen om de onder hen berustende reisdocumenten, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreemding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins".

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

3.1.3 Rijbewijzen

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

De artikelen 122 tot en met 130 van het Reglement Rijbewijzen hebben betrekking op de eisen aan de beveiliging rondom de uitgifte van rijbewijzen. Zo wordt geëist dat de met afgifte van rijbewijzen belaste autoriteiten zorg dragen voor een op schrift gestelde beveiligingsprocedure, met daarin in ieder geval beveiligingsvoorschriften ten aanzien van: toegang van personen tot en het beheer van rijbewijzen, de met de afgifte van rijbewijzen verband houdende materialen, apparatuur, toegangspassen en gebruikerscodes tot de apparatuur, de verantwoordelijkheden van de beveiligingsfunctionaris en de functiescheiding.

3.2 Periodieke zelfevaluatie, onderzoek en accountantscontrole

3.2.1 Zelfevaluatie

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

3.2.3 Onderzoek BRP gegevens

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

3.2.4 Onderzoek BRP processen

Gemeenten moeten periodiek zelf onderzoeken of zij voldoen aan de eisen die de wetgever stelt op het gebied van beveiliging en privacy bij de uitvoering van de BRP-werkzaamheden. Deze controle voert de gemeente uit aan de hand van een digitale vragenlijst BRP die RvIG via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt. De vragenlijst moet jaarlijks vóór 31 december definitief zijn ingevuld.
De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingscoördinator en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan de het college van B&W. Deze ondertekent de rapportage en stuurt deze vóór 14 februari 2022 naar RvIG.
De beveiligingsfunctionaris neemt kennis van zowel de resultaten van deze jaarlijkse zelfevaluatie en houdt toezicht op de te ondernemen acties op geconstateerde tekortkomingen.

3.2.5 Onderzoek Paspoorten en NIK

Sinds april 2013 gebruiken gemeenten voor haar onderzoek naar reisdocumentenproces de vragenlijst in de Kwaliteitsmonitor van RvIG. Dit instrument moet verplicht gebruikt worden voor de evaluatie van het reisdocumentenproces en moet jaarlijks vóór 31 december definitief zijn ingevuld.

De managementrapportage die de Kwaliteitsmonitor genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsfunctionaris reisdocumenten en voorzien van een actieplan van de gemeente) ter kennis worden gebracht aan de het college van B&W. Het bestuursorgaan, de burgemeester, ondertekent de rapportage en stuurt deze vóór 14 februari 2022 naar RvIG.
De beveiligingsfunctionaris reisdocumenten neemt kennis van zowel de resultaten van deze jaarlijkse zelfevaluatie en houdt toezicht op de te ondernemen acties op geconstateerde tekortkomingen.

3.2.6 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 zouden de maatregelen zoals genoemd in artikel 128 lid 1 van dit reglement jaarlijks onderdeel uit moeten maken van de accountantscontrole.

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

3.3 Taken, verantwoordelijkheden en bevoegdheden

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

Op het gebied van de Waardedocumenten dienen te worden aangewezen een beveiligingsfunctionaris reisdocumenten, de Autorisatie Bevoegde Reisdocumenten, de beveiligingsfunctionaris rijbewijzen en de Autorisatie Bevoegde Rijbewijzen.

De beschrijving en toekenning van de rollen in het kader van de Waardedocumenten maken deel uit van de bijlagen. Voor alle in dit hoofdstuk voorkomende functies is in de bijlage Functieverdeling de vervanging vastgelegd.

3.4 Functiescheiding Waardedocumenten

Om de kans te verkleinen dat medewerkers van de afdeling Burgerzaken 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; bij de aanvraag van een reisdocument moet een foto- en handtekeningformulier worden gebruikt. Eventueel kan daarbij een aanvraagformulier worden ingevuld.
- Beheer: Hieronder wordt verstaan de verantwoordelijkheid voor de materialen en (gepersonaliseerde) waardedocumenten tussen het moment van de aanvraag en de uitreiking.
- Uitreiking: Hieronder wordt verstaan het feitelijk aan de houder ter beschikking stellen van het op zijn naam gestelde waardedocument.

3.4.1 Functiescheiding Reisdocumenten

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

- Tussen de beveiligingsfunctionaris reisdocumenten en degenen die belast zijn met uitvoerende- en beheertaken met betrekking tot reisdocumenten (artikel 93, lid 10 PUN).
- 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 (artikel 93 lid 1, sub c PUN). Het reisdocument moet door een andere medewerker worden uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

De functiescheiding op dit gebied wordt in de gemeente Lingewaard bereikt doordat op het aanvraagformulier de paraaf van de medewerker is geplaatst, die over de aanvraag heeft beslist.
- Door de medewerkers wordt er middels de signalering in de reisdocumentenmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt.
- Voorts dient er ingevolge artikel 93, lid 1, sub c PUN functiescheiding te zijn gerealiseerd tussen degene die het beheer heeft over de voorraad gepersonaliseerde reisdocumenten en de medewerkers die de aanvraag behandelen dan wel de uitreiking verzorgen.

Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Zie procedure Ontbreken van voldoende functiescheiding.

Hierbij gelden op grond van artikel 93, lid 3 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.

3.4.2 Functiescheiding Rijbewijzen

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

Tussen aanvraag en uitreiking van rijbewijzen
Het rijbewijs wordt door een andere medewerker uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

De functiescheiding op dit gebied wordt in de gemeente Lingewaard bereikt doordat op het aanvraagformulier de paraaf van de medewerker is geplaatst, die over de aanvraag heeft beslist. Door de medewerkers wordt er middels de signalering in de rijbewijsmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt.
Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Zie procedure Ontbreken van voldoende functiescheiding.

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

Schriftelijk wordt vastgelegd:

- De reden waarom tijdelijk niet aan de eis van functiescheiding kan worden voldaan;
- De periode waarin niet aan de eis van functiescheiding kan worden voldaan;
- De namen van de ambtenaren, die in deze periode zijn belast met de aanvraag, het beheer en de uitreiking van de rijbewijzen.

Bijlagen: procedures, rapportages en bijlagen.

Lingewaard, 21 maart 2023

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

De burgemeester,
dr. P.T.A.M. Kalfs

De secretaris,
drs. I.P. van der Valk

Burgemeester in haar hoedanigheid als verantwoordelijke voor het onderdeel Waardedocumenten.

De burgemeester,
dr. P.T.A.M. Kalfs

Bijlage 1 Regeling beheer en toezicht Basisregistratie Personen (BRP)

Het College van B&W van de gemeente Lingewaard,

Gelet op de:

- Wet basisregistratie personen (Wet BRP);
- Verordening Gegevensverstrekking BRP;
- Nadere regeling Gegevensverstrekking BRP;
- Algemene verordening gegevensbescherming (AVG),

besluiten:

vast te stellen de navolgende regeling beheer en toezicht BRP voor de gemeente Lingewaard.

1. AANWIJZEN FUNCTIONARISSEN

Artikel 1
Het College van B&W van de gemeente Lingewaard wijst functionarissen aan die belast worden met:

1 Het informatiebeheer
2 Het gegevensbeheer
3 Het systeembeheer
4 Het functioneel applicatiebeheer
5 Het privacybeheer BRP
6 De gegevensverwerking
7 De toezichthouders
8 Het beveiligingsbeheer
9 Het namens het College van B&W van de gemeente Lingewaard afnemen van de in artikel 2.8, lid 2, onder sub e, van de wet BRP bedoelde verklaring

2. HET INFORMATIEBEHEER

Artikel 2
De informatiebeheerder beheert de voorziening voor de BRP , de gegevensmakelaar/datadistributie gegevensmakelaar en het autorisatiebesluit.

Artikel 3
De informatiebeheerder voorziet in:

a. Een jaarlijkse planning van de beheeractiviteiten.
b. Een jaarlijkse rapportage aan het College van B&W over de bij punt a bedoelde planning, waarbij tevens inzicht wordt gegeven in de kengetallen van de bijhoudings- en beheerprocedures.
c. Een jaarlijkse rapportage over de resultaten die voortvloeien uit de in artikel 12 bedoelde kwaliteitssteekproef.
d. Administratieve beheerprocedures, voor zover hierin niet door of bij de wet is voorzien.
e. Periodiek overleg tussen hem-/haarzelf en de op basis van de regeling aangewezen beheerders.
f. Richtlijnen voor de bijhouding van de BRP.

Artikel 4
De informatiebeheerder is verantwoordelijk voor:

a. De uitvoering van het periodieke onderzoek op grond van artikel 4.3 van de Wet BRP, naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie.
b. De periodieke toezending van een uittreksel van de resultaten van het onderzoek aan de Autoriteit Persoonsgegevens en aan de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

Artikel 5
De informatiebeheerder adviseert het College van B&W over de navolgende aspecten die voortvloeien uit deze basisregistratie te weten:

a. Persoonsinformatievoorziening
b. Beveiliging
c. Gegevenskwaliteit

d. Personeelsaangelegenheden

Artikel 6
De informatiebeheerder beslist:

a. Over de installatie van nieuwe of gewijzigde versies van de applicatie.
b. Op verzoeken van organen van de gemeente tot het verkrijgen van gegevens uit de BRP.
c. Op verzoeken van derden als genoemd in artikel 3.6 van de Wet BRP, en derden als genoemd in de Verordening gegevensverstrekking BRP tot het verkrijgen van gegevens uit de BRP.
d. Over de wijze van de verstrekking van gegevens [1] met betrekking tot het bepaalde in dit artikel onder b en c.

Artikel 7
De informatiebeheerder ziet erop toe dat:

a. De in deze regeling opgenomen bepalingen worden nageleefd.
b. De behandeling en afhandeling van verzoeken om gegevensverstrekking als genoemd in artikel 7 geschiedt volgens de bepalingen uit de Wet BRP, de Verordening gegevensverstrekking BRP en de AVG.
c. De bij of krachtens de wet opgelegde verplichtingen worden nageleefd ten aanzien van inrichting en bijhouding, evenals de beveiliging van de voorziening voor de BRP.
d. Dat alle in artikel 2 genoemde functionarissen op de hoogte zijn van de installatie van nieuwe of gewijzigde versies van de applicatie voor de voorziening voor de BRP, en van de gevolgen van deze installatie.
e. De beveiligingsvoorschriften worden nageleefd die voortvloeien uit het informatiebeveiligingsbeleid, het informatiebeveiligingsplan en de bijbehorende procedures en werkinstructies.

Artikel 8
De informatiebeheerder, of een op grond van artikel 1 aangewezen functionaris, neemt deel aan interne en externe overleggen betreffende onderwerpen die het beheer van de voorziening voor de BRP aangaan.

3. HET GEGEVENSBEHEER

Artikel 9
1 De gegevensbeheerder is verantwoordelijk voor:
   a. De juistheid, actualiteit en betrouwbaarheid van de gegevens die opgenomen zijn of worden in de voorziening voor de BRP.
   b. Het beheer van documentatie op het gebied van de wet en overige regelgeving op het gebied van de BRP.
   c. De communicatie met de overheidsorganen aan wie gegevens worden verstrekt uit de BRP, en de communicatie over gegevensverwerking met andere houders van voorzieningen voor de BRP.
   d. Het verwerken van complexe mutaties en correcties met betrekking tot de BRP.
   e. Het uitzetten van richtlijnen met betrekking tot het actualiseren en corrigeren van persoonsgegevens in de voorziening voor de BRP.

2 De gegevensbeheerder beslist binnen vijf werkdagen over het in behandeling nemen van een melding van een overheidsorgaan dat gerede twijfel heeft over de juistheid van een in de voorziening van de BRP opgenomen (authentiek) gegeven, en stelt het overheidsorgaan in kennis van deze beslissing.

Artikel 10
De gegevensbeheerder voorziet in:

a. De behandeling van wijzigingsverzoeken zoals bedoeld in artikel 2.57, 2.58 en 2.60 van de Wet BRP.
b. Controlewerkzaamheden ter waarborging van de kwaliteit van de BRP.

Artikel 11
De gegevensbeheerder is bevoegd om, in overleg met de applicatiebeheerder, vanuit de in artikel 10 bedoelde verantwoordelijkheid de gegevensverwerkers aanwijzingen te geven betreffende de opname en bijhouding van gegevens in de voorziening voor de BRP.

1) Verstrekkingsmogelijkheden zijn: ad hoc vragen op persoon of adres, mutatieberichten op papier of via de gegevensmakelaar/data-distributie, en selectieverstrekkingen.

Artikel 12

1 Periodiek wordt de inhoudelijke kwaliteit van het bestand van persoonslijsten in de BRP onderworpen aan een inhoudelijke controle door de Minister van BZK.
2 De gegevensbeheerder voorziet in een doorlopende kwaliteitssteekproef en de uitvoering van de daarmee samenhangende verbetermaatregelen, gericht op de handhaving van de kwaliteitsnorm van het ministerie van BZK.
3 De gegevensbeheerder neemt deel aan het in artikel 3 onder e genoemde overleg.

Artikel 13

De gegevensbeheerder voorziet in de uitvoering van het periodiek onderzoek op grond van artikel 4.3 van de Wet BRP, voor wat betreft de verwerking van persoonsgegevens in een voorziening.

4. HET SYSTEEMBEHEER

Artikel 14

De systeembeheerder is verantwoordelijk voor het technisch onderhoud van de bedrijfsapplicatie waarmee een voorziening voor de BRP wordt gevoerd (hierna applicatie).

Artikel 15

De systeembeheerder voorziet in:

a. De fysieke beveiliging van de applicatie.
b. Een dagelijkse back-up die wordt ondergebracht in een daartoe uitgeruste en beveiligde ruimte op een andere locatie dan de ruimte waarin de apparatuur voor een voorziening van de BRP is opgesteld.
c. De technische installatie van gewijzigde of nieuwe versies van de applicatie .
d. De beschikbaarheid van de applicatie , overeenkomstig hetgeen daarover intern en met derden is overeengekomen.

Artikel 16

De systeembeheerder is bevoegd om:

a. Direct maatregelen te treffen wanneer de continuïteit van de applicatie of de daarin opgeslagen informatie acuut in het geding is; de systeembeheerder is verplicht om achteraf terzake te rapporteren aan de informatiebeheerder.
b. Aanwijzingen te geven over:
    i. het beheer van toepassingssystemen;
    ii. het beheer van bestanden;
    iii. reconstructiemaatregelen.

Artikel 17

De systeembeheerder neemt deel aan het in artikel 3 onder e genoemde overleg.

5. HET FUNCTIONEEL APPLICATIEBEHEER

Artikel 18

De functioneel beheerders voorziet in:

a. De communicatie bij storingen in hard- en software.
b. Een logboek waarin bijzondere gebeurtenissen worden bijgehouden.
c. De toekenning van de autorisatieniveaus voor actualiseringen aan de gegevensverwerkers, de gegevensbeheerder, en de functioneel beheerders zelf op grond van een besluit van de informatiebeheerder.
d. De bijhouding van een dossier van autorisaties die door de informatiebeheerder zijn toegekend.
e. Het testen en evalueren van nieuwe versies van de applicatie , alsmede het testen en evalueren van nieuwe apparatuur.
f. De beoordeling van de gevolgen van de installatie van nieuwe en of gewijzigde versies van de applicatie .
g. De bijhouding van een verzameling van alle problemen en klachten die bij het gebruik van de applicatie ontstaan.
h. Een oplossing, eventueel door inschakeling van de systeembeheerder of een derde, voor de onder g genoemde problemen en klachten.
i. De voorlichting aan alle in artikel 1 genoemde functionarissen met betrekking tot de gevolgen van een nieuwe of gewijzigde versie van de applicatie .
j. De coördinatie van de werkzaamheden in geval van uitwijk, in overleg met de systeembeheerder.
k. De vormgeving en inhoud van documenten die rechtstreeks aan de BRP worden ontleend.

l. De afhandeling van verzoeken omtrent managementgegevens.
m. Een zo spoedig mogelijke oplossing in geval van storingen binnen de applicatie , zo nodig door inschakeling van een derde.

Artikel 19
De functioneel beheerders is verantwoordelijk voor:

a. De ondersteuning bij het gebruik van de applicatie .
b. Het tijdig opschonen van de relevante bestanden in de database.
c. Het beheer van de tabellen van de BRP.
d. Het beheer van de gebruikersdocumentatie.

Artikel 20
De functioneel beheerders is bevoegd om:

a. Gegevensverwerkers en het personeel van externe organisatieonderdelen/-diensten, die direct toegang hebben tot de BRP, aanwijzingen te geven over het gebruik van de applicatie .
b. Gedragsregels op te stellen over het gebruik van de BRP.

Artikel 21
De functioneel beheerders is verantwoordelijk voor de gehele of gedeeltelijke uitvoering van de uitwijkprocessen zoals beschreven in de procedure uitwijk van het informatiebeveiligingsplan.

Artikel 22
De functioneel beheerders ziet erop toe dat voorgeschreven procedures uit het informatiebeveiligingsbeleid, het informatiebeveiligingsplan en de bijbehorende procedures en werkinstructies worden nageleefd.

Artikel 23
De functioneel beheerders neemt deel aan:

a. Het overleg genoemd in artikel 3 onder e.
b. Het externe gebruikersoverleg.

6. HET PRIVACYBEHEER

Artikel 24
1 de privacy officer adviseert de medewerkers van het Klant Contact Centrum, de informatiebeheerder en het College van B&W over de privacyaspecten die voortvloeien uit de uitvoering van de wet BRP en de Verordening gegevensverstrekking BRP.
2 de privacy officer is verantwoordelijk voor:
   a. De advisering over de inhoudelijke afhandeling van de verzoeken zoals bedoeld in artikel 6, onder b, c en d van deze regeling.
   b. Het dagelijkse toezicht op de naleving van de privacyvoorschriften in relatie tot het gebruik van gegevens uit de BRP die voortvloeien uit de wet BRP en de AVG.

Artikel 25
de privacy officer adviseert over:

a. De afhandeling van verzoeken om inzage in de BRP overeenkomstig artikel 2.55 van de wet BRP.
b. De behandeling van alle verzoeken om verstrekkingsbeperking die op basis van artikel 2.59 van de wet BRP ingediend worden, en van de eventuele privacytoets als bedoeld in artikel 3.21 lid 2 van de wet.
c. De afhandeling van verzoeken ingevolge de artikelen 12 tot en met 21 van de AVG.
d. De kennisgeving ingevolge de rechten van betrokkene(n) zoals vermeld in hoofdstuk III van de AVG.
e. De afhandeling van verzoeken om inzage in verstrekkingen uit de BRP aan overheidsorganen en derden.

Artikel 26
de privacy officer is bevoegd om:

a. Op grond van het in artikel 25 sub 2b genoemde toezicht, alle gebruikers van gegevens uit de BRP aanwijzingen te geven.

b. Ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de BRP, waarbij de persoonlijke levenssfeer in het geding is.

Artikel 27
de privacy officer is betrokken bij alle bezwaarschriftenprocedures die voortvloeien uit genomen beslissingen op grond van de Wet BRP, de daarbij behorende regelingen en de AVG voor zover hierbij privacyaspecten aan de orde zijn.

7. DE GEGEVENSVERWERKING

Artikel 28
De gegevensverwerkers voorzien in:

a. Het verwerken van de gegevens in de BRP overeenkomstig de voorschriften van de krachtens de wet BRP voorgeschreven systeembeschrijving en de handleiding uitvoeringsprocedures (HUP), voor zover ze daartoe door de applicatiebeheerder zijn geautoriseerd.
b. Het verzamelen van de daarvoor bestemde gegevens.
c. De archivering van de brondocumenten op grond waarvan de gegevens zijn verwerkt.
d. De behandeling van mutaties.
e. De behandeling van het netwerkverkeer.
f. De behandeling van de foutverslagen die voortvloeien uit de inkomende netwerkberichten.
g. De toetsing van de waarde die aan overgelegde brondocumenten kan worden toegekend aan de hand van artikel 2.8 van de wet BRP. Daarnaast zien ze erop toe dat geen gegevens worden verwerkt uit documenten waaraan bij of krachtens de Wet BRP geen ontleningstatus is gegeven.
h. De dagelijkse controle van de in de BRP aangebrachte actualiseringen.
i. De kennisgeving aan de ingeschrevene voor wat betreft de verwerking van:
    i. wijziging van het naamgebruik;
    ii. vervolginschrijving, voor zover het een adreswijziging betreft die leidt tot opname in de BRP.

j. De toezending van de persoonslijst aan de ingeschrevene in geval van een inschrijving in de BRP.
k. De afhandeling van de verzoeken om inzage in de BRP overeenkomstig artikel 2.55 van de wet BRP (inzage), de behandeling van alle verzoeken om verstrekkingsbeperking die op basis van artikel 2.59 van de wet BRP ingediend worden, en de eventuele privacytoets als bedoeld in artikel 3.21 lid 2 van de wet BRP.
l. De afhandeling van verzoeken ingevolge de artikelen 12 tot en met 21 van de AVG.
m. De kennisgeving ingevolge de rechten van betrokkene(n) zoals vermeld in hoofdstuk III van de AVG.
n. De afhandeling van verzoeken om inzage in verstrekkingen uit de BRP aan overheidsorganen en derden.

Artikel 29
De gegevensverwerkers:

a. Beslissen op aangiften en verzoekschriften die op grond van de wet worden gedaan met inachtneming van het gestelde in artikel 25 en voor zover hierin niet op andere wijze is voorzien.
b. Beslissen over het verwerken van resultaten van onderzoeken die zijn ingesteld naar aanleiding van een melding van een overheidsorgaan.
c. Stellen overheidsorganen in kennis van de beslissing ingevolge sub b. van dit artikel.

8. DE TOEZICHTHOUDER

Artikel 30
De toezichthouders als bedoeld in artikel 4.2 van de Wet BRP zijn verantwoordelijk voor het toezicht op de naleving van de verplichtingen van de burger ingevolge hoofdstuk 2, afdeling 1, paragraaf 5 van de Wet BRP.

Artikel 31
De toezichthouder controleert of de burger aan zijn verplichtingen voldoet met betrekking tot de inschrijving in de BRP (artikel 2.38), de wijziging van diens adres (artikel 2.39), het rechtmatig gebruik van een briefadres (artikelen 2.40 t/m 2.42), zijn vertrek uit Nederland (artikel 2.43), en de verstrekking van alle inlichtingen die nodig zijn voor de bijhouding van de BRP.

Artikel 32

De toezichthouder ziet er op toe dat—indien de burger niet zelf aan zijn verplichtingen voldoet of kan voldoen—de verplichtingen worden vervuld door degene die daartoe bevoegd is op grond van de artikelen 2.49 en 2.50 van de Wet BRP.

Artikel 33

1 De toezichthouder ontleent de in lid 2 van dit artikel genoemde bevoegdheden aan hoofdstuk 5 van de Algemene Wet Bestuursrecht.

2 De toezichthouder is in verband met de uitvoering van de taken als genoemd in artikel 31, bevoegd om:

a. Met uitzondering van het zonder toestemming van een bewoner betreden van een woning, elke plaats te betreden met meeneming van apparatuur (zoals laptop, fotocamera).
b. Zich zo nodig toegang verschaffen met behulp van de sterke arm.
c. Zich te laten vergezellen door personen die door hem zijn aangewezen.
d. Inlichtingen te vorderen.
e. Inzage te vorderen van een identiteitsbewijs.
f. Zakelijke gegevens te vorderen, kopieën te maken of documenten mee te nemen om te kopiëren.
g. Onderzoek te doen.
h. Rapport op te maken inzake een geconstateerde overtreding van de bepalingen van de Wet BRP, als genoemd in artikel 31.

Artikel 34

De toezichthouder voert zijn werkzaamheden uit in samenspraak met de gegevensverwerker en koppelt het resultaat van zijn werkzaamheden terug aan de gegevensverwerker.

Artikel 35

1 De toezichthouder is bevoegd om namens het College van B&W een bestuurlijke boete op te leggen.

2 De toezichthouder neemt bij gebruik van de bevoegdheid als bedoeld in lid 1 van dit artikel binnen de gemeente Lingewaard ter zake geldende beleidsregels in acht.

Artikel 36

De toezichthouder legt het resultaat van zijn werkzaamheden vast in een onderzoekrapportage en draagt zorg voor dossiervorming.

9. HET BEVEILIGINGSBEHEER

Artikel 37

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

2 De CISO is in het bijzonder verantwoordelijk voor het opstellen en uitvoeren van het plan Informatiebeveiligingsbeleid, voor de voorzieningen waarmee de gemeente Lingewaard uitvoering geeft aan de Wet BRP en voor het gegevensmagazijn.

Artikel 38

1 De CISO ondersteunt en adviseert de informatiebeheerder op het gebied van het informatiebeveiligingsbeleid, op zodanige wijze dat de informatiebeheer diens verantwoordelijkheid op grond van de artikelen 3 en 5 van dit reglement op deugdelijke wijze kan invullen.

2 De CISO coördineert de uitvoering van de beveiligingsmaatregelen van het plan Informatiebeveiligingsbeleid.

Artikel 39

De CISO is bevoegd om:

a. Uit hoofde van diens verantwoordelijkheid als bedoeld in artikel 38 alle gebruikers van gegevens uit de BRP aanwijzingen te geven.
b. Ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de BRP waarbij de beveiliging in het geding is.

Artikel 40

De CISO:

a. Onderkent en reageert op incidenten, en adviseert over de maatregelen die nodig zijn om de gevolgen van een incident te beperken en om herhaling te voorkomen.
b. Stelt passende normen en controlemaatregelen op.

c. Implementeert beveiligingsmaatregelen.
d. Coördineert en handhaaft de uitvoering van de maatregelen als genoemd onder c.

Artikel 41
De CISO is het aanspreekpunt op het gebied van informatiebeveiligingsbeleid en bevordert het beveiligingsbewustzijn bij management en medewerkers.

Artikel 42
De CISO:

a. Neemt deel aan het in artikel 3 onder e genoemde overleg.
b. Participeert in de ontwikkeling en formulering van het informatiebeveiligingsbeleid.

Artikel 43
De CISO rapporteert jaarlijks over de informatieveiligheid aan de informatiebeheerder en verzorgt de bijdragen aan de managementrapportage over de informatieveiligheid met betrekking tot de persoonsinformatievoorziening.

Artikel 44
De CISO is verantwoordelijk voor het toezicht op naleving van de beveiligingsmaatregelen en –procedures met inachtneming van de door alle gemeenten overgenomen Baseline Informatiebeveiligingsbeleid Gemeenten (BIG) en Baseline Informatiebeveiligingsbeleid Overheid (BIO).

Artikel 45
De CISO is bevoegd om het management dwingende adviezen te geven ten aanzien van de naleving van de beveiligingsvoorschriften die voortvloeien uit de Wet BRP en de BIG/BIO.

Artikel 46
De CISO ziet er op toe dat:

a. Beveiligingsvoorschriften die voortvloeien uit de Wet BRP en het informatiebeveiligingsbeleid worden nageleefd.
b. De in deze regeling opgenomen bepalingen inzake beveiliging worden nageleefd.

Artikel 47
De CISO adviseert rechtstreeks aan het College van B&W over beveiligingsaspecten die uit het informatiebeveiligingsbeleid voortvloeien.

Artikel 48
De CISO voorziet in een jaarlijks verslag over de activiteiten inzake het beveiligingsbeheer van de BRP.

10. SLOTBEPALINGEN

Artikel 49
De in deze regeling opgenomen bepalingen gelden voor de voorzieningen zoals bedoeld artikel 1.2 juncto 1.4 van de Wet BRP, evenals voor de in de voorziening genoemde aangehaakte gegevens en voor de basisgegevens uit de BRP in het gegevensmagazijn.

Artikel 50
Deze regeling treedt in werking op de eerste dag na die waarop zij is bekend gemaakt.

Artikel 51
Deze regeling wordt aangehaald als 'Regeling beheer en toezicht basisregistratie personen de gemeente Lingewaard'.

Aldus besloten in de vergadering van het College van B&W van 21 maart 2023.

Lingewaard,

Het College van B&W van de gemeente Lingewaard,

dr. P.T.A.M. Kalfs, burgemeester

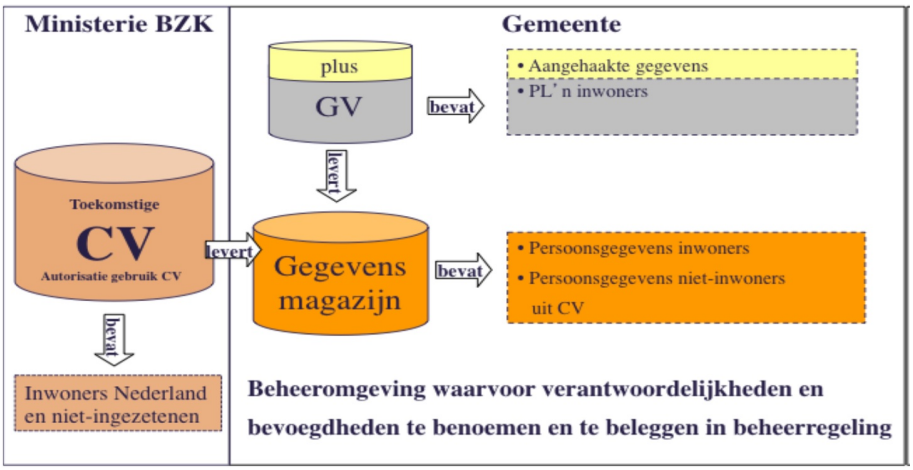
drs. .I.P .van der Valk , gemeentesecretaris

Toelichting op de Regeling beheer en toezicht BRP

Sinds 1 januari 2010 geldt voor de hele overheid, en dus ook binnen gemeenten, de verplichting om bij de uitvoering van taken gebruik te maken van persoonsgegevens uit de basisadministratie persoonsgegevens (GBA), thans basisregistratie personen (BRP). Organisatieonderdelen (volgens de wet 'organen') van de gemeente (voorheen afnemers) dienen gegevens over de personen met wie ze zaken doen te betrekken uit de BRP.

Op grond van artikel 4.15 van de Wet BRP mag de gemeente tot aan het moment dat ze overgaat op het gebruik van een nieuwe BRP-voorziening, gebruik blijven maken van het GBA-systeem waarmee ze werkte tot aan het moment van inwerkingtreding van de Wet BRP. In aansluiting op artikel 4.15 van de Wet BRP wordt in deze regeling de term 'voorziening voor de uitvoering van de BRP' gebruikt, in deze toelichting afgekort tot BRP. In de BRP registreert de gemeente gegevens over haar inwoners.

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is op grond van artikel 1.9 van de Wet BRP verantwoordelijk voor de centrale voorzieningen waarmee de Wet BRP wordt uitgevoerd. De centrale voorzieningen (afgekort CV) zullen gegevens gaan bevatten over alle personen die in Nederland woonachtig zijn (ingezetenen) en over personen die niet in Nederland wonen, maar die wel een relatie hebben met de Nederlandse overheid (niet-ingezetenen). Vooralsnog zal de minister aan de Wet BRP uitvoering geven met behulp van de reeds bestaande landelijke voorziening voor de BRP, de GBA-V, en met een voorziening voor registratie voor de niet-ingezetenen (RNI).



Figuur 1

Voor het gebruik van persoonsgegevens uit de BRP kunnen nadere regels worden gesteld, bij of krachtens Verordening. De verkrijging van gegevens uit de BRP is gebaseerd op een autorisatiebesluit van de minister van BZK.

In de praktijk vindt distributie van persoonsgegevens doorgaans niet (meer) rechtstreeks plaats vanuit de BRP, maar vanuit een specifiek daarvoor ingericht gegevensmagazijn. Dat gegevensmagazijn wordt gevoed vanuit zowel de BRP (inwoners) als vanuit de (toekomstige) centrale voorziening (voor de niet-inwoners en niet-ingezetenen). Het hiervoor beschrevene wordt geïllustreerd in Figuur 1.

Beheer én toezicht
Uit oogpunt van privacy, beveiliging, beheer en toezicht is het noodzakelijk voor de BRP om een aantal taken te benoemen en vast te leggen in een regeling waarin de hoofdlijnen van het beheer van en toezicht op de BRP is geregeld. Los van de noodzaak verplicht ook de wetgever het College van B&W via artikel 1.11 van de Wet BRP om zich te houden aan de nadere regels van de systeembeschrijving (Logisch Ontwerp GBA). Het Logisch Ontwerp schrijft in hoofdstuk 8 de aanwijzing door het College van B&W voor van functionarissen die een aantal beheertaken uitvoeren. Deze hebben alleen betrekking op de BRP.

De regeling is formeel gezien bedoeld voor de gegevensverwerking in de BRP. Op de gegevens van inwoners en niet-inwoners in het gegevensmagazijn is de AVG van toepassing. De verwerking van de uit de BRP afkomstige gegevens met behulp van het gegevensmagazijn dient te worden opgenomen in het AVG-verwerkingsregister.

Desondanks is het van belang om uit oogpunt van eenheid van persoonsinformatie- en privacybeleid én van de beheersbaarheid van de informatiestromen ook de voor het gegevensmagazijn relevante beheeraspecten onder te brengen, respectievelijk te integreren, in de regeling voor de BRP. Daarmee

ontstaat een 'regeling voor informatievoorziening basisgegevens', die zowel betrekking heeft op het beheer van de BRP als op het gegevensmagazijn.

Verdeling beheer- en toezichtrollen
Deze regeling onderkent naast een aantal beheerrollen—te weten informatiebeheer, gegevensbeheer, applicatiebeheer, technisch beheer, beveiligingsbeheer en privacybeheer—ook de rol van de gegevensverwerker, toezichthouder en controller informatiebeveiliging.

Gegevensverwerkers verwerken uitsluitend de persoonsgegevens voor de BRP. De inhoudelijke verantwoordelijkheid voor de basisgegevens van personen die niet tot de bevolking van de gemeente worden gerekend, ligt namelijk bij de beheerder van de BRP's van de andere gemeenten en bij de beheerder van de centrale voorzieningen, de Minister van BZK.

De verdeling van de beheer- en toezichtrollen is mede afhankelijk van de inrichting van de (persoons)informatiehuishouding en het informatie- en beveiligingsbeleid van de gemeente. De taken, verantwoordelijkheden en bevoegdheden per rol en de bijbehorende competenties zijn richtinggevend voor de plaats in de organisatie waar deze belegd worden. Rollen kunnen worden gecombineerd zoals de security officer BRP, de beveiligingsfunctionaris Reisdocumenten en Rijbewijzen, beveiligingsfunctionaris Reisdocumenten en Rijbewijzen, de privacy officer, de privacy officer.

Beveiligingsbeheer
De inhoud van de rol van de beveiligingsbeheerder had onder het regime van de GBA vooral betrekking op toezichtaspecten. Voor een correcte uitvoering van beveiligingsbeheer en -toezicht (en tevens voor aansluiting op de BIG/BIO) is het noodzakelijk gebleken om de inhoud van beheer en toezicht in aparte rollen onder te brengen. De regeling bevat nu in hoofdstuk 9 het beveiligingsbeheer.

Privacybeheer
De privacy officer adviseert de informatiebeheerder over alle privacyvraagstukken aangaande de persoonsgegevensverwerking waarvoor de informatiebeheerder verantwoordelijk is. Daarnaast adviseert de privacy officer degenen die belast zijn met de dagelijkse uitvoering van de werkzaamheden in het kader van de Wet en Verordening BRP.

De taken van de privacy officer beperken zich in deze regeling niet tot de verwerking van persoonsgegevens uit de BRP. Verzoeken uit de organisatie om gegevens uit zowel de BRP als uit de centrale voorzieningen, dienen door de privacy officer getoetst te worden op doelbinding, rechtmatigheid, proportionaliteit, et cetera. Daaronder valt ook de advisering over de wijze van verstrekking van gegevens uit de BRP, en over koppelingen tussen het gegevensmagazijn en de verschillende systemen van de gebruikers in de organisatie. De privacy officer adviseert de informatiebeheerder, die moet beslissen bij dergelijke verzoeken. Een verzoek kan inhouden dat men gebruik wil maken van de bestaande ministeriële autorisatie, maar ook uitbreiding van de autorisatie in verband met de uitvoering van een taak die nog niet in het autorisatiebesluit is voorzien. De rol van de privacy officer kan worden gecombineerd met de security officer BRP.

Leeswijzer Regeling beheer en toezicht BRP

- Het eerste hoofdstuk van de Regeling beheer en toezicht BRP betreft de aanwijzing van de functionarissen die worden belast met de verschillende beheer- en toezichtrollen. Het College van B&W wijst de functionarissen aan wiens inhoudelijke rol zich niet beperkt tot de BRP of het gegevensmagazijn.
  Gelet op de noodzaak van een onafhankelijke rolinvulling, wijs het College van B&W de privacybeheerder BRP aan.

  De informatiebeheerder voorziet in de aanwijzing van het functioneel inhoudelijk beheer, het verstrekkingenbeheer uit de BRP en het gegevensmagazijn. De informatiebeheerder als bronhouder beheert de inhoud en de kwaliteit van de gegevens in de BRP en stelt tevens leveringsvoorwaarden (i.c. privacyvoorwaarden) aan de verstrekking van gegevens uit de BRP.

  De gegevensverstrekking binnen de gemeentelijke organisatie over niet-inwoners uit de BRP dient gebaseerd te zijn op het autorisatiebesluit van de minister van BZK. Het beheer en de uitvoering van dat autorisatiebesluit maken deel uit van het functioneel inhoudelijk en verstrekkingenbeheer.
- De hoofdstukken 2 tot en met 9 bevatten de taken, verantwoordelijkheden en bevoegdheden per rol.
- De slotbepalingen zijn opgenomen in hoofdstuk 10.

Bijlage 1 Aanwijzing van beheerfunctionarissen
Op grond van artikel 1 van de BRP-beheerregeling zijn de navolgende beheerfunctionarissen aangewezen:

Informatiebeheer
Als informatiebeheerder is aangewezen de teammanager KCC.

Gegevensbeheer
Als gegevensbeheerder is aangewezen Wilma Kuster, Carolien Hegeman en Joyce Berns. (zij vervangen elkaar hierin).

Applicatiebeheer
Als functioneel beheerders voor de applicatie is aangewezen Sander van de Weerd..

Er is geen plaatsvervanger aangewezen.

Naast de applicatiebeheerder zijn tevens belast met het berichtenverkeer:
- Medewerkers Frontoffice en Backoffice Burgerzaken.

de privacy officer BRP
Als privacy officer is aangewezen Rachel Peters.

Haar plaatsvervanger is Sander van de Weerd.

de systeembeheerder
Als systeembeheerder is aangewezen Henri de Wit. .
Als zijn plaatsvervanger is aangewezen Marc de Ruiter en Werner Muller.

Gegevensverwerking
Als gegevensverwerkers worden alle medewerkers van het team Burgerzaken aangewezen. Zij vervangen elkaar hierin.

Toezicht
Als toezichthouders BRP zijn aangewezen: (zij vervangen elkaar hierin).

- Fayssal Hamdaoui,
- Patricia Verburgt-Wieland,
- Wilma Kersten,
- Marjo van Zagten,
- Dorie Pattinasarany,
- Wilma Kuster,
- Kai Huisman,
- Jeannette Starmans
- Bob Bruil,
- Carolien Hegeman,
- Joyce Berns.

de privacy officer (AVG)
Als privacy officer is aangewezen Yvonne Behet.

de Beveiligingbeheerder
Als Beveiligingsbeheerder (CISO) is aangewezen Eric-Hans Bais.

Als beveiligingsbeheerder BRP (ISO) is aangewezen Rachel Peters en Sander van de Weerd.

de beveiligingsfunctionaris reisdocumenten/rijbewijzen
Als beveiligingsfunctionaris Waardedocumenten is aangewezen Rachel Peters en Eric-Hans Bais.

Afnemen verklaringen artikel 2.8, lid 2 van de wet
De bevoegdheid tot het namens het college van burgemeester en wethouders afnemen van de in artikel 2.8, lid 2, onder sub e, van de wet bedoelde verklaring (afnemen van de verklaring onder ede of belofte) wordt toegekend aan:
- Alle medewerkers Publiek 1