MEIERIJSTAD
GEMEENTEBLAD
Officiële uitgave van de gemeente Meierijstad
Nr. 56761
9 februari
2022

Informatiebeveiligingsplan BRP en waardedocumenten

Gebaseerd op de wet, besluit en regeling BRP, de Paspoortwet en Paspoort Uitvoeringsregeling Nederland en het reglement Rijbewijzen.

1. Inleiding

Voorwoord

In de Wet basisregistratie personen (BRP), de Paspoortwet en het Reglement Rijbewijzen stelt de wetgever eisen aan de beveiliging van de uitvoeringsprocessen voor de BRP en waardedocumenten. De processen BRP en waardedocumenten zijn echter niet de enige bedrijfsprocessen waarvoor beveiliging noodzakelijk is zoals voorgeschreven in de voornoemde wetten. De gemeente verwerkt op tal van plaatsen in de organisatie gegevens over personen, waarvoor de Algemene Verordening Gegevensbescherming (AVG) de gemeente Meierijstad verplicht tot het treffen van beveiligingsmaatregelen. Ook buiten het domein van de persoonsgegevens valt er nog heel wat te beveiligen; bijvoorbeeld rond besluitvormingsprocessen waarbij de gemeente Meierijstad als belanghebbende nadeel kan ondervinden als het besluit te vroeg in de openbaarheid komt.
Een organisatiebreed informatiebeveiligingsbeleid met daarop afgestemde plannen is noodzakelijk om de totale bedrijfsvoering van de gemeente Meierijstad te beveiligen. Dit strategische informatiebeveiligingsbeleid van Meierijstad wordt elke 3 jaar door de CISO opgesteld en door het College vastgesteld. De hierin opgenomen algemene beveiligingsmaatregelen zijn afgestemd op de inhoud van de Baseline Informatiebeveiliging Overheid (BIO).
Dit informatiebeveiligingsplan BRP en waardedocumenten is een uitwerking van het strategische informatiebeveiligingsbeleid specifiek gericht op het domein van de BRP en waardedocumenten.

Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt en als alle actoren die daarbij een rol hebben, hier op een juiste manier invulling aan geven. Beleidsdoelstellingen bepalen het informatiebeveiligingsbeleid; een informatiebeveiligingsplan is gericht op de implementatie van het beleid. Binnen de organisatie moeten medewerkers verantwoordelijkheden krijgen ten aanzien van de uitvoering van het plan.
Medewerkers worden (onder andere tijdens het werkoverleg) betrokken bij de implementatie van het beleid. Zij zijn immers medeverantwoordelijk voor de uitvoering van het informatiebeveiligingsplan.
De CISO stelt vast of de genomen maatregelen ook worden nageleefd.
Het informatiebeveiligingsplan BRP en waardedocumenten wordt jaarlijks door de beveiligingsbeheerder BRP en de beveiligingsfunctionaris reisdocumenten en rijbewijzen geëvalueerd en beoordeeld op basis van het beleid en de beleidsuitgangspunten. Waar nodig wordt het plan bijgesteld. Het bevat immers een stelsel van procedures en maatregelen voor de dagelijkse praktijk, inclusief afspraken over de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen en procedures. Dat moet getoetst worden op actualiteit.

Verantwoording

Wijzigingen die direct betrekking hebben op individuele taken en bevoegdheden worden expliciet en rechtstreeks door de leidinggevende naar de betrokken medewerker(s) gecommuniceerd. Alle medewerkers van de gemeente Meierijstad worden
via de reguliere interne kanalen door hun leidinggevende geïnformeerd over de wijzigingen die voor hen van belang zijn in het informatiebeveiligingsbeleid, het -plan, de -maatregelen en/of de -procedures.
Jaarlijks overhandigt de werkgroep informatiebeveiliging het aangepaste plan rechtstreeks ter advisering aan de gemeentesecretaris en het directieteam. Daarna wordt het ter vaststelling aangeboden aan de bevoegde bestuursorganen, het college van B&W respectievelijk de burgemeester.

2. Informatiebeveiliging

Informatiebeveiliging

'Informatiebeveiliging' is de verzamelnaam voor de processen die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen, en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Informatiebeveiliging heeft betrekking op:

- Beschikbaarheid / continuïteit: ervoor zorgen dat informatie en informatie verwerkende bedrijfsmiddelen voor gebruikers beschikbaar zijn op de juiste tijd en plaats.
- Integriteit / betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en van informatieverwerking.
- Vertrouwelijkheid / exclusiviteit : het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor diegenen die ertoe geautoriseerd zijn.

Informatiebeveiligingsbeleid

De gemeente Meierijstad stelt elke 3 jaar een strategische informatiebeveiligingsbeleid op dat door het College van B&W wordt vastgesteld. Dit informatiebeveiligingsplan BRP en waardedocumenten is een uitwerking van dit beleid specifiek op het domein BRP en waardedocumenten. In dit plan staan de domein specifieke doelstellingen en uitgangspunten vermeld.

Raakvlakken met ander beleid

Het informatiebeveiligingsbeleid heeft onder meer raakvlakken met het beleid en met de daaruit voortvloeiende procedures die gericht zijn op de operationele veiligheid van het uitgifte- en beheerproces van waardedocumenten. Het informatiebeveiligingsbeleid inzake de BRP en waardedocumenten valt onder het organisatiebrede strategisch informatiebeveiligingsbeleid. Binnen het beleidsterrein Informatiebeveiliging kan onderscheid worden gemaakt tussen fysieke, logische en organisatorische beveiligingsmaatregelen. Voorbeelden hiervan zijn identificatie van gebruikers, sleutelbeleid, personeelsbeleid en een clean desk clear screen-policy.

Beleidsdoelstellingen

De gemeente Meierijstad 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 maatregelen richten zich in ieder geval op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens, en op de controleerbaarheid van de gemeentelijke bedrijfsprocessen. Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het bestuur van de gemeente Meierijstad 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 kennen van minimaal 97% tijdens werktijden. Buiten werktijden worden er geen eisen gesteld aan de beschikbaarheid, met uitzondering van voorzieningen in het kader van rampenbestrijding.

Wettelijk kader verwerking persoonsgegevens

De Algemene Verordening gegevensbescherming (AVG) vormt het algemeen kader voor de verwerking van persoonsgegevens. De verplichting tot beveiliging van persoonsgegevens is geregeld in artikel 5, lid 1 onder f van de AVG.

De Autoriteit Persoonsgegevens (AP) kan de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens, bij gemeenten het college van B&W of de burgemeester, aanspreken op het niveau van de maatregelen ter beveiliging van de verwerking van persoonsgegevens, en op de wijze waarop het stelsel van maatregelen is geïmplementeerd en wordt nageleefd.

Buiten het algemeen kader van de AVG dient het college van B&W 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. Voor dit plan is relevant dat de AVG niet van toepassing is, voor wat betreft de verwerking van persoonsgegevens in de BRP. De beveiliging van de BRP is geregeld bij en krachtens de Wet BRP.

Verantwoordelijkheden, bevoegdheden en taken

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 BRP adviseert de CISO over de inrichting en organisatie van het informatiebeveiligingsbeleid op het gebied van de persoonsinformatievoorziening en ziet erop toe dat de beveiligingsvoorschriften worden nageleefd die voortvloeien uit de wet en het informatiebeveiligingsplan.

De beveiligingsbeheerder BRP is verantwoordelijk voor het opstellen en actualiseren van het Informatiebeveiligingsplan voor de gemeentelijke voorzieningen en voor het gegevensmagazijn waarmee de gemeente Meierijstad uitvoering geef aan de Wet BRP.

De CISO controleert periodiek de realisatie en/of naleving van de beveiligingsmaatregelen en -procedures van het plan Informatiebeveiliging BRP en waardedocumenten (zie Beheerregeling Basisregistratie personen (BRP)).

Verantwoordelijkheden van het bestuur

Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Meierijstad. Het college van B&W stelt in dit plan het onderdeel Informatiebeveiliging BRP vast en de burgemeester het onderdeel waardedocumenten.

Genoemde bestuursorganen onderschrijven volledig de beveiligingsmaatregelen die in dit plan Informatiebeveiliging BRP en waardedocumenten worden voorgeschreven. Ze 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 de uitgifte van waardedocumenten heeft de burgemeester op basis van de Paspoortwet en het Reglement Rijbewijzen de uiteindelijke verantwoordelijkheid.

Verantwoordelijkheden van het directieteam

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle leden van het directieteam van de gemeente Meierijstad. Het directieteam bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.
Per jaar zullen de volgende punten met betrekking tot beveiliging aan de orde komen:

- voortgang van de realisatie van beveiligingsmaatregelen, zoals beschreven in het Informatiebeveiligingsplan BRP en waardedocumenten en gerapporteerd door de beveiligingsbeheerder BRP;
- mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen;
- bespreking van, en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingsfunctionaris reisdocumenten en rijbewijzen;
- goedkeuring van initiatieven om de (informatie)beveiliging te verbeteren;
- het geven van voor iedereen zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen;
- het bevorderen van het beveiligingsbewustzijn;
- herziening en goedkeuring van het beveiligingsbeleid en van de toegekende verantwoordelijkheden.

Verantwoordelijkheden CISO
De CISO is op gemeentelijk niveau verantwoordelijk voor de informatiebeveiliging. De CISO is verantwoordelijk voor:

- het opstellen en periodiek actualiseren van het integrale informatiebeveiligingsbeleid, -plan en -maatregelen;
- coördinatie van, en toezicht op de uitvoering van het integrale informatiebeveiligingsbeleid;
- het periodiek (laten) uitvoeren van risicoanalyses ten aanzien van het integrale informatiebeveiligingsbeleid;
- afstemming met beveiligingsbeheerders van de verschillende domeinen, waaronder de beveiligingsbeheerder BRP en de beveiligingsfunctionaris reisdocumenten en rijbewijzen.

De CISO zal gevraagd en ongevraagd adviseren over de informatiebeveiliging van de gemeente Meierijstad. De CISO zal de totstandkoming van de rapportages coördineren; de uitkomsten analyseren en evalueren; voorstellen doen ter verbetering van de informatiebeveiliging en toezien op de uitvoering en naleving van maatregelen op het gebied van informatiebeveiliging.
Verantwoordelijkheden beveiligingsbeheerder BRP
Om de continuïteit en actualiteit van informatiebeveiliging inzake de BRP en waardedocumenten te borgen, is de rol van de beveiligingsbeheerder in het leven geroepen. De beveiligingsbeheerder BRP adviseert over de inrichting en organisatie van het informatiebeveiligingsbeleid, specifiek met betrekking tot de BRP en waardedocumenten. Tevens heeft de beveiligingsbeheerder BRP de verantwoordelijkheid om namens de bestuursorganen toe te zien op naleving van de beveiligingsmaatregelen en -procedures, zoals uitgewerkt in het Informatiebeveiligingsplan BRP en waardedocumenten. De beveiligingsbeheerder BRP rapporteert daarover aan het college van B&W respectievelijk de burgemeester.
De beveiligingsbeheerder BRP toetst periodiek het Informatiebeveiligingsplan BRP en waardedocumenten aan het beleid, alsmede de consistentie tussen het plan enerzijds en de uitvoering en naleving van de beveiligingsmaatregelen en -procedures anderzijds.
De functie van beveiligingsbeheerder BRP moet niet verward worden met de functie van de beveiligingsfunctionaris reisdocumenten en rijbewijzen. Deze laatstgenoemde functie kent zeer specifieke taken en verantwoordelijkheden op het beveiligingsgebied van enerzijds de reisdocumenten en anderzijds de rijbewijzen.
Verantwoordelijkheden beveiligingsfunctionaris reisdocumenten en rijbewijzen
De beveiligingsfunctionaris reisdocumenten en rijbewijzen is verantwoordelijk voor:

- De controle (steekproefsgewijs) op de naleving van de beveiligingsprocessen, -procedures en instructies betreffende reisdocumenten mede aan de hand van de normeringen uit de zelfevaluatie PNIK;
- De controle op een juiste afhandeling van de zelfevaluatie PNIK;
- Het (laten) verrichten van onderzoek bij beveiligingsincidenten met het doel dergelijke situaties in de toekomst te voorkomen;
- Het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten en/of tekortkomingen in de beveiligingsvoorzieningen.

Daarnaast kent de beveiligingsfunctionaris reisdocumenten en rijbewijzen de volgende algemene beveiligingstaken, met betrekking tot reisdocumenten en rijbewijzen, waarvoor zij/hij tevens verantwoordelijk is:

- Het bewaken van uit te voeren acties voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van het Informatiebeveiligingsplan BRP en waardedocumenten;
- Het toezicht houden op de actualiteit van het Informatiebeveiligingsplan BRP en waardedocumenten, de beveiligingsprocessen, -procedures/afspraken en instructies;
- Gevraagd en ongevraagd advies geven aan de burgemeester en het managementteam over verbeteringen ten aanzien van de beveiliging;

- Het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures;
- Het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en –processen;
- Het toezicht houden of (nieuwe) medewerkers worden geïnstrueerd en bekendgemaakt met de beveiligingsprocedures en –processen met betrekking tot reisdocumenten;
- Het registreren van de meldingen van beveiligingsincidenten;
- Het rapporteren aan de burgemeester betreffende de stand van zaken van beveiliging, eventueel naar aanleiding van bijzonderheden/incidenten;
- Het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

Verantwoordelijkheden van overige rollen / functies
De verantwoordelijkheden van de rollen en/of functies van de gegevensbeheerder, privacybeheerder, applicatiebeheerder, systeembeheerder en beveiligingsbeheerder zijn vastgelegd. Voor alle in het Informatiebeveiligingsplan BRP en waardedocumenten voorkomende functies is in de Beheerregeling Basisregistratie personen (BRP) de vervanging vastgelegd. De aanwijzing van de beveiligingsfunctionaris reisdocumenten en rijbewijzen is hierin niet opgenomen. Dit is een apart aanwijzingsbesluit wat genomen wordt door de burgemeester.
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 door 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 voor de betrokkene bestaan 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 Meierijstad.
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 die verbonden zijn aan de gedefinieerde risicoklasse. De te nemen maatregelen worden gewogen aan de hand van de volgende criteria:
- Risico's - zowel van de verwerking, als ook van de aard en de omvang van de persoonsgegevens.
- De stand van de techniek.
- Kosten.

3. Kwaliteitsaspecten
Inleiding
Het strategische informatiebeveiligingsbeleid omvat een verzameling van strategische uitgangspunten. Hierin maken de bestuurlijke en ambtelijke top eendrachtig duidelijk aan het tactische en operationele niveau welke gedragslijn in de gemeente Meierijstad gevolgd moet worden om tot een adequate informatiebeveiliging te komen. Het beleid vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Het op- en vaststellen van een informatiebeveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten uit het informatiebeveiligingsbeleid concreet worden toegepast door middel van maatregelen. Aan de hand van periodieke controles op de uitvoering stelt het directieteam vervolgens vast of de maatregelen werken.
Evaluatie van het beleid moet periodiek plaatsvinden om na te gaan of het beleid nog steeds aansluit op de organisatie.
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 gegevensverwerking.
2. Integriteit - De persoonsgegevens moeten in overeenstemming zijn met 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 de 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 zijn gestructureerd en gebruikt.

De gemeente Meierijstad hanteert voor deze kwaliteitsaspecten de vier hieronder beschreven normen voor het domein BRP en waardedocumenten.

Norm voor beschikbaarheid

Het college van B&W en het directieteam zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening wordt gestaakt, als gevolg waarvan een aantal bedrijf kritische applicaties niet meer kunnen functioneren. Dit geldt in het bijzonder (maar niet uitsluitend) voor de informatievoorziening met betrekking tot de BRP.

Voor onze bijzonder persoonlijke dienstverlening is het van cruciaal belang dat de informatiesystemen/voorzieningen die de BRP en WD processen ondersteunen, tijdens de openingstijden voor het publiek beschikbaar zijn. Daarom dienen deze systemen/voorzieningen op jaarbasis voor 100% beschikbaar te zijn tijdens de openingstijden voor het publiek.

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

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 niet realistisch als concrete eis. Ten behoeve van 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.

Een gemeente voldoet aan de norm als minder dan het hieronder aangegeven normpercentage aan bevindingen is geconstateerd.

1. Algemene Gegevens (Burgerlijke Staat)	A. Persoon en Overlijden		(2 %)	✔
	B. Adres		(2 %)	✔
	C. Relaties		(3 %)	✔
2. Algemene Gegevens (overig)	D. Identificatienummers en nationaliteit		(4 %)	✔
	E. Overig algemeen		(4 %)	✔
3. Administratieve Gegevens	F. Administratief		(5 %)	✔
4. Brondocument	G. Niet aanwezig		(5 %)	✔
TOTAAL				✔

Norm voor vertrouwelijkheid

Uitsluitend bevoegde personen in dienst van of werkzaam voor de gemeente hebben toegang tot de voor hen relevante gegevens in registraties. De bevoegdheid van een persoon moet worden afgeleid van diens taak; dit is ter beoordeling van de informatiebeheerder BRP, op aangeven van de direct leidinggevende van de betreffende persoon.

Iedere medewerker binnen de gemeente die inzage heeft in persoonsgegevens of belast is met het bijhouden van BRP-gegevens en/of werkt met waardedocumenten, dient een geheimhoudingsverklaring te hebben ondertekend.

Norm voor controleerbaarheid

Mutaties in persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente Meierijstad reiken. Toelating tot Nederland is bijvoorbeeld 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 ook dat—gelet op mogelijke belangenverstrengeling—gecontroleerd moet kunnen worden wie welke mutatie heeft verwerkt. De gemeente Meierijstad kent als norm dat 99% van alle mutaties in persoonsgegevens herleidbaar moeten zijn tot de individuele persoon die voor de mutatieverwerking verantwoordelijk was, en dat zulks geldt voor 90% van alle raadplegingen.

3.6 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. 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 het voorliggende document Informatiebeveiligingsplan BRP en waardedocumenten opgenomen procedures hebben als doel te voorkomen dat de risico’s zich voordoen die horen bij de aan de verwerking van persoonsgegevens verbonden risicoklasse (II). Uitvoering van de procedures maakt het bedrijfsproces controleerbaar uit oogpunt van beveiliging.

4. Wettelijke verplichtingen

Verplichtingen vanuit de 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 van beschikbaarheid (continuïteit), integriteit (betrouwbaarheid), vertrouwelijkheid (exclusiviteit) en controleerbaarheid.
De gemeente moet op grond van de Wet BRP de beveiligingsmaatregelen nemen die die wet voorschrijft. Als grondslag voor het beveiligingsplan op het onderdeel BRP zijn de artikelen 1.10 en 1.11 Wet BRP van belang.
Artikel 1.10 bepaalt dat de beveiligingsmaatregelen BRP bij of krachtens Algemene Maatregel van Bestuur (AMvB) worden geregeld (het Besluit BRP). Artikel 1.11 draagt het college van B&W op om zich aan die maatregelen te houden.

Besluit BRP

Gelet op het belang voor het informatiebeveiligingsplan volgt hieronder de tekst van artikel 6 Besluit BRP. Wet BRP en Besluit BRP gaan verder in het stellen van eisen aan de beveiliging dan de AVG. Bovendien geldt op grond van artikel 4.3 Wet BRP de verplichting om jaarlijks uiterlijk op 31 december conform de ENSIA-verantwoordingssystematiek zelf onderzoek te doen naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie.
Artikel 6 Besluit BRP

1. Het college van B&W 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.

Verplichtingen Reisdocumenten

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

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

Verplichtingen 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 reisdocumenten en rijbewijzen;
- De functiescheiding.

Periodieke zelfevaluatie, onderzoek en accountantscontrole

4.1.1. Zelfevaluatie

De in het Informatiebeveiligingsplan BRP en waardedocumenten voorgestelde beveiligingsmaatregelen en - procedures vormen voor een groot deel het object van onderzoek bij de jaarlijkse zelfevaluaties PNIK en BRP, voorgeschreven door de Paspoortwet en de Wet BRP.
De uitslagen van de zelfevaluaties worden naar de Rijksdienst voor Identiteitsgegevens (RvIG) gezonden—door het college van B&W voor wat betreft de BRP, en door de burgemeester voor wat betreft de reisdocumenten. Vervolgens worden ze openbaar gemaakt via de webapplicatie Kwaliteitsmonitor. Die kwaliteitsmonitor is er ook voor de controle op de inhoudelijke kwaliteit van de gegevens. Vanaf 2017 wordt dit gecombineerd met de ENSIA-verantwoordingssystematiek.

4.1.2. Onderzoek BRP gegevens

De 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. Met behulp van een persoonlijke log-in kan elke gemeente in het onderdeel 'Monitor Gegevens' de resultaten bekijken van de BRP-onderdelen die op haar betrekking hebben. De gegevens in de BRP moeten voldoen aan de kwaliteitsnormen die op grond van artikel 47 Besluit BRP bij Ministeriële regeling worden bepaald.

4.1.3. 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 RvIG via de Kwaliteitsmonitor aan gemeenten beschikbaar stelt en een vragenlijst binnen de ENSIA-tool. Deze vragenlijsten moeten 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 beveiligingsbeheerder en voorzien van een actieplan van de gemeente) worden aangeboden aan het college van B&W. Het college ondertekent het bijbehorende uittreksel en stuurt deze vóór 15 februari naar de RvIG en de Autoriteit Persoonsgegevens (AP).
De beveiligingsbeheerder BRP neemt kennis van de resultaten van deze jaarlijkse zelfevaluatie en houdt toezicht op de te ondernemen acties.

4.1.4. Onderzoek Paspoorten en NIK

Ook voor hun onderzoek naar het reisdocumentenproces gebruiken gemeenten de vragenlijst in de Kwaliteitsmonitor van de 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) worden aangeboden aan de burgemeester. Het bestuursorgaan, de burgemeester, ondertekent het bijbehorende uittreksel en stuurt deze vóór 15 februari naar de RvIG en de AP.
De beveiligingsfunctionaris reisdocumenten en rijbewijzen neemt kennis van de resultaten van deze jaarlijkse zelfevaluatie en houdt toezicht op de te ondernemen acties.

4.1.5. Accountantscontrole Rijbewijzen

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

Eventuele tekortkomingen die bij de jaarlijkse evaluatie van het beheerproces rond waardedocumenten (reisdocumenten en rijbewijzen) worden geconstateerd, worden schriftelijk vastgelegd. De daarop betrekking hebbende rapportages worden vijf jaar bewaard. Op de eventueel geconstateerde tekortkomingen wordt actie ondernomen.

Taken, verantwoordelijkheden en bevoegdheden

Op grond van of krachtens de wet BRP, de Paspoortwet en het Reglement Rijbewijzen dienen een aantal taken, verantwoordelijkheden en bevoegdheden te worden vastgelegd en in de organisatie belegd. Zolang de gemeente de wet BRP uitvoert met de lokale voorzieningen die de Wet GBA voorschreef, betreft dit de beheerrollen die betrekking hebben op het informatiebeheer, het gegevensbeheer, het privacybeheer, het applicatiebeheer en het systeembeheer. Op het gebied van de waardedocumenten dienen te worden aangewezen:

- De beveiligingsfunctionaris reisdocumenten
- De autorisatiebevoegde reisdocumenten
- De beveiligingsfunctionaris rijbewijzen
- De autorisatiebevoegde rijbewijzen

Functiescheiding installatie

- Alleen geautoriseerd personeel kan functies en software installeren of activeren.

Functiescheiding Waardedocumenten

Om de kans te verkleinen dat medewerkers van het atelier 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 volgt een korte uitleg van de relevante termen:

- Aanvraag/verstrekking: 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: De verantwoordelijkheid voor de materialen en (gepersonaliseerde) waardedocumenten tussen het moment van de aanvraag en de uitreiking.
- Uitreiking: Het feitelijk aan de houder ter beschikking stellen van het op zijn naam gestelde waardedocument.

Functiescheiding Reisdocumenten

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

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

De functiescheiding tussen aanvraag en uitreiking wordt in de gemeente Meierijstad bereikt doordat het uitreiken gedaan wordt door de medewerkers van het KCC.

Middels het instellen van een beperking in de reisdocumentenmodule wordt bereikt dat de uitreiking niet kan plaats vinden door de medewerker die ook de aanvraag heeft gedaan.

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. Hierbij gelden op grond van artikel 93, lid 3 van de PUN voorschriften.

Schriftelijk wordt vastgelegd:

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

De uitdraai uit het RAAS en de afschriften van de in deze periode verstrekte documenten worden afzonderlijk bewaard.

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

Functiescheiding Rijbewijzen

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

- 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 tussen aanvraag en uitreiking wordt in de gemeente Meierijstad bereikt doordat het uitreiken gedaan wordt door de medewerkers van het KCC.
Middels het instellen van een beperking in de rijbewijsmodule wordt bereikt dat de uitreiking niet kan plaats vinden door de medewerker die ook de aanvraag heeft gedaan.
Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken. Hierbij gelden op grond van artikel 128, lid 3 van het Reglement Rijbewijzen de volgende voorschriften.
Schriftelijk wordt vastgelegd:

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

De betreffende aanvraagformulieren en de gegevens over de in deze periode verstrekte documenten worden afzonderlijk bewaard.
Na afloop van de betreffende periode controleert de beveiligingsfunctionaris rijbewijzen of de schriftelijke vastlegging aanwezig is en of de aanvraag, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

4.11.Functiescheiding Suwinet

Verder is er een bijzonder strikte functiescheiding geregeld bij de gemeente Meierijstad ten aanzien van Suwinet, vanwege de bijzonder privacygevoelige gegevens die zijn vastgelegd in deze landelijke registratie.
Bij functiescheiding is vastgelegd dat de volgende taken bij verschillende personen zijn belegd:

- De uitvoering van taken (het gebruik van Suwinet).
- Het beheer van autorisaties (toegang verlenen tot Suwinet). Dit wordt uitgevoerd door de functioneel beheerder Suwinet.
- Kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet) wordt uitgevoerd door de beveiligingsbeheerder Suwinet.
- Management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen van het belang van goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet).

5. Procedures behorend bij dit informatiebeveiligingsplan

Vakgebied BRP

5.1.1. Procedure beoordelen van brondocumenten
5.1.2. Procedure inschrijven in de BRP
5.1.3. Procedure actualiseren van gegevens
5.1.4. Procedure corrigeren van gegevens
5.1.5. Procedure controle op volledigheid, juistheid en actualiteit gegevens
5.1.6. Procedure verwijderen van gegevens
5.1.7. Procedure verstrekkingsbeperking
5.1.8. Procedure onderzoek juistheid van de gegevens
5.1.9. Procedure protocolleren
5.1.10. Procedure terugmeldingen
5.1.11. Procedure verstrekken van gegevens
5.1.12. Procedure inzagerecht BRP
5.1.13. Procedure reconstructie van data en gegevens BRP
5.1.14. Procedure opleggen bestuurlijke boete
5.1.15. Procedure adresonderzoek
5.1.16. Procedure evaluatie maatregelen BRP
5.1.17. Procedure data Integriteit BRP
5.1.18. Procedure extern gebruik BRP
5.1.19. Procedure briefadres

Vakgebied waardedocumenten (rijbewijzen)

5.1.20. Procedure aanvragen van rijbewijzen
5.1.21. Procedure verzenden van aanvragen rijbewijzen
5.1.22. Procedure ontvangst en transport van rijbewijzen en overige materialen
5.1.23. Procedure bewaren van rijbewijzen en overige materialen
5.1.24. Procedure uitreiken en vernietigen van rijbewijzen
5.1.25. Procedure vermissing van rijbewijzen
5.1.26. Procedure bijzondere procedures rijbewijzen

Vakgebied waardedocumenten (reisdocumenten)
5.1.27. Procedure identiteit vaststellen en machtigen
5.1.28. Procedure aanvragen van reisdocumenten
5.1.29. Procedure ontvangst en transport van reisdocumenten en overige materialen
5.1.30. Procedure verzenden van aanvragen reisdocumenten
5.1.31. Procedure bewaren en beheren van reisdocumenten en overige materialen
5.1.32. Procedure uitreiken en vernietigen van reisdocumenten met koerier
5.1.33. Procedure vermissing van reisdocumenten
5.1.34. Procedure van rechtswege vervallen documenten
5.1.35. Procedure voorraadbeheer
5.1.36. Procedure afwijking in de voorraad
5.1.37. Procedure functiescheiding Waardedocumenten
5.1.38. Procedure fysieke beveiliging van het RAAS en (mobiele) aanvraagstations
5.1.39. Procedure technische beveiliging van het informatiesysteem
5.1.40. Procedure registratie van de afgifte van identificatiekaart, pincode en wijzigingscode
5.1.41. Werkinstructie van rechtswege vervallen documenten
5.1.42. Procedure evaluatie maatregelen PNIK

Vaststelling

Voor accordering van het voorliggend plan Informatiebeveiliging BRP en waardedocumenten tekent hieronder de opdrachtgever.
Dit Informatiebeveiligingsplan treedt in werking na vaststelling door het college van B&W. Hiermee komt het oude Informatiebeveiligingsplan BRP en waardedocumenten, vastgesteld op 02-02-2021, te vervallen.

Aldus vastgesteld door burgemeester en wethouders van gemeente Meierijstad op 01-02-2022.
De secretaris,
mevrouw M.G.C. Wilms-Wils
De burgemeester,
de heer C.H.C. van Rooij,