

Beveiligingsrichtlijn basisregistratie personen, reisdocumenten en rijbewijzen

Dit document is een aanvulling op het informatiebeveiligingsbeleid gemeente Haaksbergen 2023-2026

1. Inleiding

1.1 Voorwoord

In de Wet basisregistratie personen, de Paspoortwet en het Reglement Rijbewijzen stelt de wetgever eisen aan de beveiliging van de uitvoeringsprocessen op het gebied van de basisregistratie personen (BRP) en de uitgifte van reisdocumenten en rijbewijzen. De BRP is een basisregistratie. Dat betekent dat deze informatie binnen de hele overheid gebruikt wordt. Bijvoorbeeld bij het verlenen van zorg, toegang tot opleidingen of toekennen van uitkeringen. Het is dus van groot belang dat de gegevens in de BRP correct zijn. Toegang tot de gegevens wordt alleen verleend als dat nodig is om een wettelijke taak uit te voeren. Bij het uitvoeren moet de privacy en de bescherming van persoonsgegevens worden geborgd.

Personen die reizen of zich moeten legitimeren doen dit met een paspoort of een identiteitskaart. Het kunnen identificeren begint bij het verstrekken van een genoemd document en is mogelijk door de registratie van persoonsgegevens. Gemeenten verstrekken paspoorten en identiteitskaarten.

In deze beveiligingsrichtlijn richten we ons op een veilig gebruik en zorgvuldige procesgang binnen de gemeentelijke organisatie op het gebied van BRP, reisdocumenten en rijbewijzen. Ook gaan we nader in op de taken, verantwoordelijkheden en bevoegdheden. De beveiligingsrichtlijn is een verdere uitwerking van het door het college vastgestelde informatiebeveiligingsbeleid 2023-2026.

1.2 Begripsbepaling

ABR	De Autorisatie Bevoegde Reisdocumenten is verantwoordelijk voor het beheer van de toegang tot het reisdocumenten aanvraag en archiefstation en het mobiele aanvraagstation
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging overheden: beschrijft het basisnormenkader voor informatiebeveiliging van overheden gebaseerd op standaarden en kwaliteitseisen
BCM	Bestandscontrole module
BRP	Basisregistratie Personen
BRP-V	BRP-Verstrekkingsvoorziening
CISO	Chief Information Security Officer
Ensia	Eenduidige Normatiek Single Information Audit
Fraude	Door kwaadwillenden worden misleid (externe fraude), of - al dan niet onder druk van chantage, bedreiging of omkoping - misbruik maken van eigen bevoegdheden (interne fraude).
FG	Functionaris Gegevensbescherming
IBB	Informatiebeveiligingsbeleid
KM-ar	Koninklijke Marechaussee
Kwaliteitsmonitor	Een systeem dat wordt gebruikt om de kwaliteit van de gegevens in de BRP te meten en te verbeteren.
LO	Logisch Ontwerp BRP
PNIK	Paspoorten en Nederlandse identiteitskaarten
PUN	Paspoort Uitvoeringsregeling Nederland
RAAS	Reisdocumenten Aanvraag- en Archiefstation
RDW	Rijksdienst voor het Wegverkeer
RYA	Functionaris die verantwoordelijk is voor het beheer van het rijbewijzen back-office station.

RvIG en BZK	Rijksdienst voor Identiteitsgegevens van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Waardedocumenten	Nederlandse identiteitsdocumenten volgens de Wet op de Identificatieplicht. Paspoort, ID-kaart en Rijbewijs.

1.3 Wettelijk kader

De volgende wet en regelgeving speelt een rol in de beveiligingsrichtlijn:

- Paspoortwet en PUN
- Circulaire verbeterimpuls identiteitsvaststelling
- Circulaire ex. Artikel 24, onder b, Paspoortwet betreffende signaleringsprocedure vermoeden misbruik reisdocumenten
- Wet BRP en regeling besluit BRP
- LO BRP
- AVG
- BIO

1.4 Periodieke aanpassing

De beveiligingsrichtlijn is geen statisch document. Binnen het vakgebied zijn er telkens wijzigingen in wet- en regelgeving, maar ook aanpassingen door bijvoorbeeld gerechtelijke uitspraken en nieuwe inzichten door de gebruikerservaringen van medewerkers. De beveiligingsrichtlijn wordt daarom eens per jaar beoordeeld op actualiteit en zo nodig aangepast.

1.5 Kaders beveiligingsbeleid

Op 6 januari 2014 is de Wet BRP in werking getreden. Gemeenten moeten op grond van de Wet BRP de beveiligingsmaatregelen nemen die de wet voorschrijft. Dit is nader uitgewerkt in het Besluit BRP. Het college moet op basis hiervan passende technische en organisatorische maatregelen treffen 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. Bovendien geldt op grond van de Wet BRP de verplichting om periodiek onderzoek te doen naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie.

De wetgever stelt daarnaast eisen aan de opslag, uitgifte en administratie van reisdocumenten. Deze eisen zijn neergelegd in de PUN. Op grond van deze regeling moeten de met de uitvoering van de Paspoortwet belaste autoriteiten maatregelen treffen 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.

Het uitgifteproces van rijbewijzen en de daarmee samenhangende beveiligingseisen komen sinds enkele jaren sterk overeen met die van reisdocumenten.

Het Reglement rijbewijzen vereist dat de met afgifte van rijbewijzen belaste autoriteiten zorg dragen voor een op schrift gestelde beveiligings-procedure, 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 betrokken functionarissen en de functiescheiding.

Controles gebeuren door de burgemeester aangestelde beveiligingsfunctionaris.

2. Beleid, verantwoordelijkheden, taken en bevoegdheden.

2.1 Onderliggend beleid en richtlijnen

Deze beveiligingsrichtlijn is een aanvulling op het gemeentelijke informatiebeleid. Dat beleid is opgesteld conform de BIO en de AVG. De baseline geeft een specifieke invulling aan de veiligheid en gebruik van informatie binnen gemeentelijke organisaties. Deze beveiligingsrichtlijn dient als algemene basis voor de verdere uitwerking van de wettelijke eisen op het gebied van BRP, reisdocumenten en rijbewijzen. De kaders zijn verder uitgediept in gedragsregels, protocollen, procedures en werkinstructies. Er wordt zo veel mogelijk gebruik gemaakt van de documenten die zijn gepubliceerd op de website van de RvIG: www.rvig.nl en de Rijksdienst voor het Wegverkeer: www.rdw.nl.

Het Handboek Burgerzaken Amsterdam van de Nederlandse Vereniging voor Burgerzaken (NVVB) is daarnaast een veel gebruikt hulpmiddel.

Goedkeuring voor gemeentelijk beleid moet altijd worden verkregen van het college van B&W voor wat betreft de BRP. En van de burgemeester voor reisdocumenten en rijbewijzen. De uitvoering, het

vaststellen van aanvullende regels en procedures is gemandateerd aan de teammanager Advies en Inwonercontacten.

2.2 Taken, verantwoordelijkheden en bevoegdheden

Op grond van de Wet BRP, de Paspoortwet en het Reglement rijbewijzen dienen een aantal taken, verantwoordelijkheden en bevoegdheden te worden vastgelegd en in de organisatie te worden belegd. De verschillende rollen en verantwoordelijkheden zijn vastgelegd in de regeling beheer en toezicht BRP gemeente Haaksbergen. De bestuurlijke verantwoordelijkheid voor de richtlijnen beveiliging BRP, reisdocumenten en rijbewijzen ligt bij het college van B&W respectievelijk de burgemeester. Deze organen laten de richtlijnen opstellen en zien toe op de uitvoering daarvan. Daarnaast kent de regeling een aantal specifieke functies zoals de applicatiebeheerder, de systeembeheerder, de gegevensverwerker en de toezichthouder.

3. Uitwerking

3.1 Kwaliteitsaspecten BRP

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 van groot belang. Het is de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten zijn gestructureerd en gebruikt.

3.2 De normen

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. Dit geldt in het bijzonder voor de informatievoorziening vanuit de BRP. Deze moet tijdens de openingstijden van het gemeentehuis maar ook daarbuiten in principe permanent beschikbaar zijn. 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 de bestuursorganen te hervatten.

Norm voor integriteit

Burgemeester en Wethouders zijn verantwoordelijk voor een actuele, juiste en betrouwbare registratie van persoonsgegevens van ingezetenen in de BRP. Daarvoor worden de nodige technische en organisatorische maatregelen getroffen, zoals bijvoorbeeld adresonderzoek. Ten behoeve van het (landelijke) 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. De registratie voldoet aan de norm als minder dan het hieronder aangegeven normpercentage aan bevindingen is geconstateerd:

Gegevenscategorie:				Norm:
1.	Algemene gegevens (burgerlijke staat)	A.	Persoon en overlijden	99,7 %
		B.	Adres	99,7 %
		C.	Relaties	99,6 %
2.	Algemene gegevens (overig)	D.	Identificatienummers en nationaliteit	99,5 %
		E.	Overig (algemeen)	99,5 %
3.	Administratieve gegevens	F.	Administratief	99,4 %
4.	Brondocument	G.	Aanwezig	99,5 %

Norm voor vertrouwelijkheid

Uitsluitend bevoegde personen in dienst van of werkzaam voor de gemeente Haaksbergen hebben toegang tot de voor hen relevante gegevens. De bevoegdheid van een persoon moet worden afgeleid

van diens taak ('need to know'). Dit ter beoordeling van de direct leidinggevende van de betreffende medewerker. Iedere medewerker binnen de gemeente legt de ambtseed of belofte af. De gemeente betracht bovendien grote terughoudendheid bij het delen van persoonsgegevens uit de BRP met externe partijen.

Norm voor controleerbaarheid

Mutaties van persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente reiken. Toelating tot Nederland is bijvoorbeeld mede afhankelijk van de nationaliteit en de 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 gecontroleerd moet kunnen worden wie welke mutatie heeft verwerkt of raadplegingen heeft gedaan. Op grond van de Wet BRP en de AVG kunnen betrokkenen deze informatie ook opvragen. De gegevens worden 20 jaar bewaard.

3.3 Verstrekken BRP gegevens

De BRP heeft primair tot doel overheidsorganen te voorzien van de opgenomen gegevens voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taken. Behalve de verstrekking van gegevens aan overheidsorganen heeft de BRP tot doel anderen te voorzien van de opgenomen gegevens in bij of krachtens de wet aangewezen gevallen. Het gaat hier binnen de basisregistratie om gevoelige persoonsgegevens, die veel zeggen over de persoonlijke levenssfeer van mensen, en daarom om maximale bescherming vragen.

Organisaties die systematisch gegevens willen ontvangen uit de BRP moeten daarvoor toestemming vragen van de minister van BZK. Zo kunnen overheidsorganen systematisch gegevens krijgen als zij deze gegevens nodig hebben voor een goede vervulling van hun taak. Dat zijn bijvoorbeeld het UWV, de Belastingdienst en de Sociale Verzekeringsbank. Ook een aantal organisaties met belangrijke maatschappelijke taken komt voor gegevensverstrekking uit de BRP in aanmerking. Het gaat daarbij om organisaties zoals pensioenfondsen, zorgverzekeraars en ziekenhuizen.

Het is ook mogelijk om voor een specifiek, eenmalig doel informatie uit de BRP te ontvangen. Er is dan sprake van incidentele verstrekking van persoonsgegevens. Dat gebeurt bijvoorbeeld als een onderzoeksinstelling persoonsgegevens nodig heeft voor wetenschappelijk onderzoek. Dat zelfde geldt voor organisaties die gerechtelijke werkzaamheden uitvoeren. Het gaat daarbij bijvoorbeeld om advocaten die gegevens nodig hebben voor rechtszaken. Dit soort organisaties wordt in de wet BRP 'verplichte derden' genoemd. Een aantal organisaties met een zogenaamd 'gewichtig maatschappelijk belang' kan eveneens in aanmerking komen voor gegevensverstrekking. Zoals advocaten, verzekeraars en banken.

Organisaties die incidenteel gegevens willen ontvangen uit de BRP kunnen daarvoor terecht bij de gemeente. Per gemeentelijke verordening is vastgelegd onder welke voorwaarden dit mogelijk is. Gemeente Haaksbergen is daarin zeer terughoudend. In alle gevallen ontvangen partijen bovendien alleen de gegevens die noodzakelijk zijn voor hun taak. Het gaat dan ook meestal om een beperkte gegevensset. De gemeente kan BRP-gegevens van haar eigen inwoners gebruiken, bijvoorbeeld voor de gemeentelijke belastingen of de gemeentelijke sociale dienst. De gemeente is verplicht deze gegevensverstrekking in de verordening vast te leggen. En ook hier geldt dat alleen de noodzakelijke gegevens worden gedeeld en uitsluitend voor publiekrechtelijke taken.

Wanneer inwoners niet willen dat hun persoonlijke gegevens aan maatschappelijke instellingen worden verstrekt, kan aan de gemeente worden gevraagd om persoonsgegevens geheim te houden.

3.4 Autorisaties

Met een autorisatie wordt bedoeld het door het management verstrekken van een gelegitimeerde toegang tot een informatiesysteem. Om toegang te krijgen tot de gegevens is naast de specifieke autorisatie voor de BRP tevens een bevoegdheid nodig op netwerk- en/of systeemniveau. De procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van medewerkers en de controle hierop. Hierbij gelden de volgende richtlijnen:

- autorisaties worden per medewerker toegekend. De autorisatie is persoonlijk en afgestemd op de functie / taken
- de bevoegdheden binnen de applicatie worden beheerd door de applicatiebeheerder
- de manager verzoekt de applicatiebeheerder de nieuwe medewerker toegang te verlenen en geven aan welke autorisatie daarbij noodzakelijk is. De applicatiebeheerder kent het autorisatieniveau toe
- bij tussentijdse wijzigingen in taken of functie verzoekt de betreffende teammanager of coördinator de applicatiebeheerder om het autorisatieniveau te wijzigen of de toegekende autorisaties in te trekken;
- bij vertrek van de medewerker worden de toegekende autorisaties direct beëindigd nadat de applicatiebeheerder een Top-desk melding krijgt

- een verzoek aan de applicatiebeheerder tot toekenning, wijziging of beëindiging gebeurt via Topdesk
- een nieuwe gebruiker krijgt van de applicatiebeheerder een melding als de autorisaties zijn geregeld.

Voor de diverse functies is behoefte aan verschillende soorten informatie en niet iedereen hoeft over alle informatie te beschikken. Alleen wat strikt noodzakelijk is voor het uitvoeren van de werkzaamheden mag worden gebruikt

Worden gegevens uit de BRP om andere redenen gebruikt, dan is er mogelijk sprake van onrechtmatig gebruik. Alleen medewerkers in dienst van de gemeente en ingehuurde externe medewerkers worden geautoriseerd. De medewerker werkt op kantoor of thuis onder gezag en toezicht van de betreffende manager. De BRP mag bij uitbesteding van taken niet worden gebruikt door medewerkers van de partij waaraan is uitbesteed.

Medewerkers van het cluster Burgerzaken beschikken over een authenticatiekaart van de RvIG, waarmee aanvragen voor reisdocumenten naar de producent kunnen worden verzonden. De pincodes zijn alleen bij de medewerker bekend en na drie onjuiste inlogpogingen wordt de kaart geblokkeerd en vervangen. De aangewezen Autorisatiebevoegde Reisdocumenten van de gemeente is bevoegd om de authenticatiekaarten te koppelen aan een medewerker en deze te ontkoppelen als een medewerker uit dienst gaat. Tevens krijgen medewerkers van het cluster Burgerzaken een door de RDW beschikbaar gestelde smartcard voor het verzenden van aanvragen voor rijbewijzen. Ook hiervoor geldt de blokkade bij drie inlog pogingen met een onjuiste pincode. De Autorisatiebevoegde Rijbewijzen zorgt namens de burgemeester voor het aanvragen, het verlengen of het intrekken van deze smartcards.

De beveiligingsfunctionaris controleert minimaal eenmaal per jaar de actualiteit en rechtmatigheid van de ingevoerde autorisaties en legt deze controle vast. De beveiligingsfunctionaris kijkt bij deze controle of het overzicht van de actieve gebruikers nog actueel is en of de bijbehorende autorisaties juist zijn. Zo nodig worden in samenwerking met de applicatiebeheerder wijzigingen doorgevoerd.

3.5 Periodieke zelfevaluatie

Jaarlijks doen gemeenten een wettelijk verplichte zelfevaluatie naar de inrichting, werking en beveiliging rondom de BRP en reisdocumenten. De zelfevaluatie, die plaatsvindt aan de hand van uitgebreide vragenlijsten, bestaat uit twee onderdelen. De zogenoemde domeinvragen gaan over de werkprocessen en zijn onderdeel van de jaarlijkse Kwaliteitsmonitor. Het betreft rechtmatigheidsvragen (Voldoen we aan wet- en regelgeving?) en volwassenheidsvragen (Wat kan er beter?). Naast de domeinvragen zijn er de informatiebeveiligingsvragen, die gaan over de inrichting en beveiliging van de verschillende systemen waarin de gegevens worden opgeslagen. De informatie-veiligheidsvragen worden door de gemeente beantwoord via de ENSIA-tool.

De deadline voor het invullen en definitief maken van de vragenlijsten is 31 december. De uittreksels met de uitkomsten van deze zelfevaluaties (eventueel voorzien van een actieplan) worden door het college van B&W voor de BRP en door de burgemeester aangaande reis-documenten ondertekend en uiterlijk 30 april verstuurd aan de Minister van BZK. Het uittreksel van de BRP gaat ook naar de AP. Het Ministerie van BZK voert steekproefonderzoeken uit naar de betrouwbaarheid van de resultaten. Nadat de gemeenten de zelfevaluatie definitief hebben ingediend, analyseert de RvIG de resultaten. Op basis van het landelijke beeld bepaalt het Ministerie de acties die het jaar na de evaluatie moeten worden ondernomen. Dit om de kwaliteit van de onderliggende processen waar nodig te kunnen verbeteren. De RvIG controleert daarnaast maandelijks de persoonslijsten in de BRP. De uitkomsten van de controles worden maandelijks aan de gemeente gerapporteerd.

Zoals eerder aangegeven, is elke gemeente wettelijk verplicht om een beveiligingsfunctionaris reisdocumenten en rijbewijzen aan te stellen. De beveiligingsfunctionaris is verantwoordelijk voor het beheer van en het toezicht op de naleving van de betreffende beveiligingsprocedures. De aanstelling gebeurt door de burgemeester, aan wie de functionaris rechtstreeks verantwoording aflegt. De bij de jaarlijkse evaluatie geconstateerde tekortkomingen worden schriftelijk vastgelegd en de daarop betrekking hebbende rapportages worden vijf jaar bewaard. De beveiligingsfunctionaris houdt toezicht op de te ondernemen acties.

3.6 Identiteit en identiteitsfraude

Er is sprake van identiteitsfraude als iemand (opzettelijk) gebruik maakt van een vals, vervalst of gestolen identiteitsdocument. Daardoor kan een ander worden benadeeld. Er zijn verschillende vormen van identiteitsfraude.

- valse documenten: niet uitgegeven door een bevoegde autoriteit

- fantasiedocumenten: fictieve documenten, dus geen bestaand model-document;
- reproductie van documenten: bijvoorbeeld een kopie
- vals opgemaakte documenten: uitgegeven door een bevoegde autoriteit op basis van onjuiste gegevens
- vervalste documenten: uitgegeven door een bevoegde autoriteit, maar later onrechtmatig gewijzigd
- vals gebruik van documenten: bijvoorbeeld 'look-alike'-fraude waarbij iemand gebruik maakt van een geldig document van een persoon op wie diegene lijkt
- onjuiste gegevens, eventueel onder eed of belofte verklaard.

Het opmaken van valse of vervalste documenten en het gebruik van deze documenten is strafbaar. Net zoals het opmaken of (opzettelijk) gebruiken van valse persoonsgegevens of biometrische kenmerken om de eigen identiteit te verhullen of een identiteit te misbruiken. Identiteitsfraude is daarbij geen doel op zich, maar kent vaak criminele, financiële, politieke of terroristische motieven. Overheden, organisaties en burgers worden hier slachtoffer van.

Het tegengaan van identiteits- en documentfraude begint bij het registreren van de juiste gegevens in de bronregistraties, zoals de BRP. Daarom moeten de processen waarin identiteitsgegevens worden vastgesteld en geregistreerd zorgvuldig zijn ingericht. Dat zelfde geldt voor de processen in het kader van de aanvraag en uitgifte van een identiteitsdocument (paspoort, rijbewijs, identiteitskaart). Met een identiteitsdocument kan in het maatschappelijke verkeer iemand zijn of haar identiteit aantonen. En dat moet kloppen. Fouten kunnen leiden tot verkeerde dienstverlening, criminaliteit en kostbare herstelacties. Alle betrokken medewerkers van de gemeente hebben de verantwoordelijkheid om vermoedelijke identiteitsfraude te signaleren en waar mogelijk te voorkomen door zorgvuldig en met kennis van zaken te handelen. De gemeente Haaksbergen volgt daarbij de landelijke ID-protocollen voor de medewerkers.

Om identiteitsfraude te voorkomen, is het belangrijk dat de processen, kunde en parate kennis van medewerkers voor het vaststellen/registreren van identiteiten en de uitgifte van identiteitsdocumenten op orde zijn. Dat vraagt om voortdurende bijscholing en adequate (technische) hulpmiddelen om identiteitsfraude te herkennen en ernaar te handelen. We nemen daarom ook deel aan de bestaande regionale contactgroepen en kwaliteitskringen. Ondersteunende diensten IND, RDW en KM-ar kunnen helpen als zij een gericht verzoek krijgen en er voorbereidend onderzoek is gedaan. Dat betekent dat medewerkers hun twijfel over een document moeten kunnen onderbouwen.

Bij een redelijk vermoeden van fraude met identiteits- of brondocumenten wordt aangifte gedaan bij de politie.

3.7 Functiescheiding reisdocumenten en rijbewijzen

Om de kans te verkleinen dat medewerkers door kwaadwillende personen 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 reisdocumenten en rijbewijzen noodzakelijk. Functiescheiding is het verdelen van taken en verantwoordelijkheden over verschillende medewerkers in de organisatie. Het Reglement rijbewijzen noemt alleen functiescheiding tussen het aanvragen en het uitreiken.

De PUN schrijft voor dat er altijd minimaal drie verschillende personen betrokken moeten zijn bij de verschillende handelingen in de aanvraag en uitgifte van paspoorten en identiteitskaarten:

- een medewerker die de identiteit van de aanvrager vaststelt en de aanvraag aanneemt
- een medewerker die de aanvraag beoordeelt en verzendt naar de producent (waarbij alleen een ambtenaar de aanvraag mag beoordelen)
- een medewerker die de identiteit van de aanvrager verifieert en het document uitreikt.

Deze functiescheiding wordt bereikt door inrichting van het werk. De aanvraag wordt in behandeling genomen door de baliemedewerker, de medewerker mid-office verzorgt de goedkeuring en verzending van de aanvraag en de medewerker receptie reikt het document uit. Daarnaast hanteren we een duidelijke functiescheiding tussen de beveiligingsfunctionaris reisdocumenten en rijbewijzen en degenen die belast zijn met de uitvoerende taken met betrekking tot aanvragen/uitreiken van deze documenten. De beveiligingsfunctionaris is buiten het team Inwonercontacten gepositioneerd om te voorkomen dat de beveiligingsfunctionaris eigen werk controleert.

3.8 Communicatie en bewustwording medewerkers

Informatieveiligheid en privacy gaat naast ICT ook om de mens in de organisatie en de manier waarop deze met risico's omgaat. Het management moet het bewustzijn van de medewerkers op het gebied van informatiebeveiliging en privacy daarom stimuleren. Dat vindt plaats door het beleid/beveiligingsrichtlijn actief uit te dragen in de organisatie. Niet alleen onder de direct bij de beveiliging betrokken medewerkers, maar bij alle mensen die in de dagelijkse praktijk bij BRP, reisdocumenten en rijbewijzen

betrokken zijn. Om de bewustwording te vergroten onder de medewerkers worden de volgende acties uitgevoerd:

- het beleid / beveiligingsrichtlijn is voor alle medewerkers op intranet beschikbaar
- in de werkoverleggen wordt periodiek stilgestaan bij het thema informatieveiligheid en een veilig gebruik van de BRP, het werkproces reisdocumenten en rijbewijzen
- tijdens de introductie van nieuwe medewerkers worden medewerkers geïnformeerd over het gebruik van privacygevoelige informatie
- periodiek worden ten aanzien van informatiebeveiliging en privacy voor de bewustwording van de medewerkers artikelen op intranet geplaatst. Onderdeel daarvan zijn e-learning, animatiefilmpjes en nieuwsbrieven
- jaarlijks worden één of meer workshops georganiseerd rondom de thema's informatie-veiligheid, privacy en het veilige gebruik van BRP, reisdocumenten en rijbewijzen
- informatieveiligheid / een veilig gebruik van BRP, reisdocumenten en rijbewijzen is een vast onderdeel van het goede gesprek met de medewerkers van het cluster Burgerzaken
- medewerkers leggen de ambtseed of belofte af.

Aldus besloten in de openbare collegevergadering van 4 november 2025

*M. (Marcel) Broekhuis
gemeentesecretaris*

*G.J. (Gerard) van den Hengel
burgemeester*

Bijlagen

Bij de informatiebeveiligingsrichtlijn horen werkprocessen die zijn gebaseerd op wet- en regelgeving en zorgen voor een uniforme werkwijze.

Algemeen

Procedure identiteit vaststellen en machtigen
Procedure back-up

BRP

Procedure inschrijven
Procedure beheersing van gegevens
Procedure terugmeldingen
Procedure verstrekken van gegevens
Procedure inzagerecht
Procedure protocolleren
Procedure autoriseren van gebruikers voor toegang tot iBurgerzaken
Procedure jaarlijkse Roadmap Burgerzaken
Procedure verwerken RPS-signalering
Procedure vervallen Nederlands reisdocument
Procedure brondocumenten

Waardedocumenten

Procedure aanvragen van reisdocumenten
Procedure uitreiken en vernietigen van reisdocumenten
Procedure ontvangst en transport van reisdocumenten en overige materialen
Procedure bewaren en beheren van reisdocumenten en overige materialen
Procedure voorraadbeheer
Procedure back-up en recovery RAAS-station
Procedure vermissing reisdocument
Procedure melden vermoeden van mogelijke fraude met een reisdocument
Procedure uitreiken en vernietigen van rijbewijzen
Procedure aanvragen van een rijbewijzen
Procedure omwisselen van een buitenlands rijbewijs
Procedure ontvangst en bewaren rijbewijzen