PUR MER END

GEMEENTEBLAD

Officiële uitgave van de gemeente Purmerend

Nr. 327925

9 juli 2026

Informatiebeveiligingsplan BRP en waardedocumenten 2026-2029

Burgemeester en wethouders en de burgemeester van de gemeente Purmerend, ieder voor zover het de eigen bevoegdheid betreft,

gelet op
- artikel 1.10 Wet BRP (basisregistratie personen), 1.11 Wet BRP en artikel 6 Besluit BRP
- hoofdstuk XII Paspoortuitvoeringsregeling Nederland 2001
- artikel 128 Reglement Rijbewijzen (RR)

B E S L U I T E N:

Bijgaand informatiebeveiligingsplan BRP en waardedocumenten 2026-2029 vast te stellen onder gelijktijdige intrekking van:
- het informatiebeveiligingsplan Basisregistratie Personen 2019-2021,
- het informatiebeveiligingsplan Reisdocumenten en Rijbewijzen 2019-2021, en
- de Beheerregeling basisregistratie personen (BRP) Purmerend.

Aldus vastgesteld in de vergadering d.d. 23 juni 2026

Purmerend,

burgemeester en wethouders van Purmerend,

de secretaris,
M.H. van der Weit

de burgemeester,
E. van Selm

de burgemeester,
E. van Selm

Informatiebeveiligingsplan BRP en waardedocumenten 2026-2029

Registratienummer: 885113
Datum: juni 2026

1. Inleiding

In de Wet basisregistratie personen (BRP), de Paspoortwet, de Paspoortuitvoeringsregeling Nederland 2001 (PUN) en het Reglement rijbewijzen (RR) stelt de wetgever eisen aan de beveiliging van de uitvoeringsprocessen voor de BRP, reisdocumenten en rijbewijzen.

De gegevens die in de BRP worden verwerkt, zijn veelal gevoelig van aard. Een adequate beveiliging van deze gegevens is daarom essentieel. Voorkomen moet worden dat onjuiste of onvolledige gegevens worden verwerkt, onbevoegden toegang krijgen tot gegevens of systemen uitvallen. Onjuiste of onvolledige informatie, misbruik van informatie of een datalek kan bij de verwerking van gegevens in de basisregistratie personen of de rijbewijzen- en reisdocumentenadministratie ingrijpende gevolgen hebben als risico's niet afdoende zijn afgedekt. Omdat de omgeving voortdurend verandert, moeten risico's en bestaande beveiligingsmaatregelen periodiek worden geanalyseerd om het vertrouwen van burgers in de overheid, de beschikbaarheid van de BRP en de betrouwbaarheid van de informatieverwerking te waarborgen.

Door het verplichte gebruik van de BRP bij de uitvoering van publiekrechtelijke taken is de BRP-applicatie voor de gemeente een onmisbare informatiebron. Bij uitval van deze applicatie zullen veel processen stagneren. Deze overwegingen, evenals de wettelijke bepalingen, hebben geleid tot het opstellen van een tactisch beveiligingsplan voor de BRP, reisdocumenten en rijbewijzen.

Dit plan beschrijft de waarborgen voor beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Het beveiligingsniveau van de BRP-processen, reisdocumenten en rijbewijzen wordt tweemaal per jaar getoetst en de resultaten worden vastgelegd in een rapportage. De getroffen beveiligingsmaat-

regelen worden beoordeeld aan de hand van de toepasselijke wet- en regelgeving. Indien nodig worden aanvullende maatregelen in dit plan opgenomen.

De reisdocumenten en rijbewijzen worden hierna gezamenlijk aangeduid als waardedocumenten. De verantwoordelijke bestuursorganen, het college van B&W voor de BRP respectievelijk de burgemeester voor de waardedocumenten, moeten jaarlijks rapporteren in hoeverre de organisatie aan deze eisen voldoet. 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, waarop ook de Algemene Verordening Gegevensbescherming (AVG) van toepassing is.

Het Gemeentelijk Informatiebeveiligingsbeleid (hierna: GIBB) geeft het algemene beleid ten aanzien van informatiebeveiliging voor de gemeente Purmerend. Op grond van artikel 90 van de PUN en artikel 128 van het RR moeten technische en organisatorische maatregelen worden getroffen om de gegevens met betrekking tot waardedocumenten te beveiligen. Dit beveiligingsplan bevat de specifieke bepalingen die daarop van toepassing zijn.

Op grond van artikelen 1.10 en 1.11 van de Wet BRP en artikel 6 van het Besluit basisregistratie personen is het college van B&W verantwoordelijk voor de gemeentelijke voorziening en voor het treffen van passende technische en organisatorische maatregelen om de basisregistratie personen te beveiligen.

2. Wettelijke verplichtingen

Verplichtingen vanuit de BRP

Het op schrift stellen van de 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 onderdeel BRP van dit beveiligingsplan zijn de artikelen 1.10 en 1.11 van de Wet BRP van toepassing:

- 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.

Deze te treffen maatregelen worden in de procedures behorende bij dit Informatiebeveiligingsplan BRP en waardedocumenten verder uitgewerkt in concrete voorschriften.

Verplichtingen Reisdocumenten

De wetgever stelt eisen aan de opslag, uitgifte en administratie van reisdocumenten. Deze eisen zijn neergelegd in de PUN. Hoofdstuk XII van deze Regeling met als onderwerp ‘beveiliging’ bepaalt in artikel 90: "De met de uitvoering van de wet belaste autoriteiten treffen maatregelen om de onder hen berustende reisdocumenten, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreemding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins.” Deze te treffen maatregelen worden in de procedures behorende bij dit Informatiebeveiligingsplan BRP en waardedocumenten verder uitgewerkt in concrete voorschriften.

Wettelijk kader verwerking persoonsgegevens

Voor dit plan zijn specifiek de Wet BRP, de Paspoortwet, de PUN en het RR van toepassing. Voor zover de Wet BRP geen specifieke regeling bevat, is de AVG onverkort van toepassing. De AVG vormt het algemeen kader voor de verwerking van persoonsgegevens. De verplichting tot het treffen van passende beveiligingsmaatregelen voor de persoonsgegevens is geregeld in artikel 32 van de AVG. De beveiliging van de BRP is geregeld bij en krachtens de Wet BRP. 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.

3. Rollen, taken, verantwoordelijkheden en bevoegdheden

In dit hoofdstuk zijn alle rollen, taken, verantwoordelijkheden en bevoegdheden beschreven m.b.t. de uitvoering van het informatiebeveiligingsplan BRP en waardedocumenten.

Rollen

- Burgemeester
- College van B&W

- Gemeentesecretaris / Algemeen Directeur
- CISO
- Gegevensbeheerder hierna genoemd gegevenseigenaar
- Beveiligingsfunctionaris BRP, rijbewijzen en reisdocumenten
- Applicatiebeheerder hierna genoemd functioneel beheerder*
- Systeembeheerder*
- Privacybeheerder BRP
- Gegevensverwerkers
- Autorisatiebevoegde reisdocumenten
- Ontvangstbevoegde waardedocumenten

*deze rollen behoeven nog nadere uitwerking.

Burgemeester
De autoriteit die bevoegd is tot het verstrekken van waardedocumenten is de burgemeester.
De bestuurlijke verantwoordelijkheid voor de waardedocumenten ligt op basis van artikel 26 lid 1 a van de Paspoortwet en artikel 27 RR bij de burgemeester. De burgemeester stelt daarom dit informatiebeveiligingsplan, op het onderdeel waardedocumenten, vast en ziet toe op de uitvoering daarvan.

Zowel de PUN als het RR verplicht de burgemeester een beveiligingsfunctionaris reisdocumenten en rijbewijzen aan te wijzen die belast is met het beheer van en het toezicht op de naleving van de beveiligingsprocedure.

Voor alle processen rond het beheer en de uitgifte van waardedocumenten draagt de burgemeester op basis van de Paspoortwet en het RR de verantwoordelijkheid.

College van B&W
De bestuurlijke verantwoordelijkheid voor de BRP ligt bij het college van B&W. Het college stelt het informatiebeveiligingsplan, op het onderdeel BRP, vast en ziet toe op de uitvoering daarvan. De Wet BRP verplicht het college niet om een beveiligingsfunctionaris BRP aan te wijzen. De wenselijkheid om een beveiligingsfunctionaris BRP aan te wijzen is echter wel aanwezig. Om deze reden wijst het college van B&W een beveiligingsfunctionaris BRP, reisdocumenten en rijbewijzen aan.

Gemeentesecretaris / Algemeen Directeur
De Gemeentesecretaris/Algemeen Directeur (GS/AD) is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid.

CISO
Voor een uitwerking van de taken en verantwoordelijkheden van de CISO wordt verwezen naar het GIBB.

Gegevenseigenaar
De verantwoordelijkheden van de gegevenseigenaar ligt bij de teammanager Burgerzaken. De verantwoordelijkheden omvat het waarborgen van de datakwaliteit, actualiteit, juistheid en betrouwbaarheid van informatie, continuïteit in dienstverlening en het naleven van privacywetgeving (zoals de AVG) en interne beleidsregels.
Nb. Voor de rol van gegevenseigenaren in de organisatie (naast de teammanager Burgerzaken) wordt verwezen naar het GIBB.

De gegevenseigenaar is op ambtelijk niveau verantwoordelijk voor de beveiliging van de BRP en waardedocumenten:
- het bewaken van de voortgang van de realisatie van beveiligingsmaatregelen zoals beschreven in dit informatiebeveiligingsplan;
- het benoemen van mogelijke ontwikkelingen die de bedrijfsinformatie kunnen bedreigen;
- bespreking van, en toezicht op (beveiligings)incidenten zoals gerapporteerd door de beveiligingsfunctionaris BRP, reisdocumenten en rijbewijzen;
- goedkeuring van initiatieven om de (informatie)beveiliging te verbeteren;
- het geven van zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen;
- het bevorderen van het beveiligingsbewustzijn;
- de herziening beveiligingsplan en de toegekende verantwoordelijkheden;
- de aanwijzing van een beveiligingsfunctionaris BRP, reisdocumenten en rijbewijzen
- het aanwijzen van een of meer functionarissen die belast zijn met de uitvoerende aspecten van de informatiebeveiliging BRP, zoals functioneel beheerder, systeembeheerder, privacybeheerder en gegevensverwerkers;

- stelt procedures en werkinstructies vast die noodzakelijk zijn op het gebied van de BRP en waardedocumenten.

Beveiligingsfunctionaris BRP, rijbewijzen en reisdocumenten
De taken van de beveiligingsfunctionaris BRP, reisdocumenten en rijbewijzen zijn gebaseerd op onder meer de Wet BRP, de Paspoortwet, PUN en het RR.

De beveiligingsfunctionaris heeft de volgende taken:
- is belast met het beheer van en het toezicht op de naleving van de beveiligingsprocedures en de zorg voor een actuele administratie en bijhouding daarvan;
- waarborgen van de integriteit en vertrouwelijkheid van persoonsgegevens die in de basisregistratie personen of de rijbewijzen- en reisdocumentenadministratie zijn opgenomen;
- toetst de beveiligingsprocedures door (aangekondigde en onaangekondigde) controles op verschillende momenten per jaar;
- controleert periodiek de logging en monitoring en naleving van alle toegangen en mutaties in de BRP en BRP-V.
- legt rechtstreeks verantwoording af aan de burgemeester en het college;
- adviseert bestuur en management over de processen en te nemen maatregelen die de kwaliteit van het proces garanderen;
- houdt rekening met de toepassing en uitvoering van (nieuwe) wet- en regelgeving;
- heeft geen uitvoerende taken op het gebied van Burgerzaken om de onafhankelijke positie te garanderen;
- zorgt voor beveiligingsprocedures en beveiligingsplan;
- brengt jaarlijks rapportage uit aan de burgemeester en het college over de resultaten van de zelfevaluatie en de voortgang;
- brengt jaarlijks rapportage uit aan de gegevenseigenaar over de resultaten;
- laat elke 4 jaar het informatiebeveiligingsplan en procedures opnieuw vaststellen en legt deze ter besluitvorming voor aan het college van B&W. Het informatiebeveiligingsplan wordt jaarlijks geëvalueerd en indien nodig aangepast, naar aanleiding van bijvoorbeeld de uitkomst van de vragenlijst zelfevaluatie reisdocumenten of (beveiligings)incidenten.

De privacybeheerder BRP
De taken van de privacybeheerder BRP zijn gebaseerd op onder meer de Wet BRP.

De privacybeheerder BRP heeft de volgende taken:
- adviseren van de gegevenseigenaar en het college van B&W over de privacyaspecten die voortvloeien uit de uitvoering van de Wet- en Verordening BRP.
- adviseren van de gegevenseigenaar over de inhoudelijke afhandeling en de wijze waarop verzoeken op grond van de BRP-verordening worden verstrekt.
- adviseren van de gegevenseigenaar over de afhandeling van de verzoeken om inzage in de Basisregistratie personen overeenkomstig artikel 2.55 van de Wet BRP respectievelijk artikel 15 van de Algemene Verordening Gegevensbescherming (inzage);
- de afhandeling 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;
- geven van aanwijzingen aan alle gebruikers van gegevens uit de BRP.
- ongevraagd advies uit brengen over alle procedures en producten die betrekking hebben op de BRP, waarbij sprake is van het in geding zijn van de persoonlijke levenssfeer.
- betrokken bij alle aan de Wet BRP gerelateerde bezwaarschriftprocedures die voortvloeien uit genomen beslissingen op grond van de Wet BRP en daarbij behorende regelingen.

NB. de taken van de privacybeheerder zijn onderverdeeld onder de coördinator Burgerzaken en de kwaliteitsmedewerker Burgerzaken. Voor tweedelijnsadvisering kan de privacybeheerder zich wenden tot de Privacy Officer van de gemeente.

De gegevensverwerkers
De gegevensverwerkers voorzien volgens de Handleiding Uitvoeringsprocedures (HUP) in:
- het verwerken van de gegevens in de BRP overeenkomstig de voorschriften van de krachtens de wet voorgeschreven systeembeschrijving (Logisch Ontwerp GBA) en de HUP, voor zover daartoe door de functioneel beheerder geautoriseerd;
- het verzamelen van de daarvoor bestemde gegevens;
- de archivering van de brondocumenten op grond waarvan de gegevens zijn verwerkt;
- de behandeling van mutaties;
- de behandeling van het berichtenverkeer;
- de behandeling van de foutverslagen, voortvloeiend uit het inkomende berichtenverkeer;

- de toetsing van de waarde die aan overgelegde brondocumenten kan worden toegekend aan de hand van artikel 2.8 van de wet BRP en ziet erop toe dat geen gegevens worden verwerkt uit documenten waaraan bij of krachtens de wet geen ontleningstatus is gegeven;
- de dagelijkse controle van de in de BRP aangebrachte actualiseringen;
- de kennisgeving aan de ingeschrevene voor wat betreft de verwerking van:
  - o wijziging van het naamgebruik;
  - o vervolginschrijving voor zover het een adreswijziging betreft die leidt tot opname in de BRP.

- de toezending van de complete persoonslijst aan de ingeschrevene ingeval van een inschrijving in de BRP;
- de afhandeling van de verzoeken om inzage in de BRP overeenkomstig artikel 2.55 van de wet BRP;
- de behandeling van alle verzoeken om verstrekkingsbeperking die op basis van artikel 2.59 van de wet BRP;
- de afhandeling van verzoeken om inzage in verstrekkingen uit de BRP aan overheidsorganen en derden;
- beslissen over het verwerken van resultaten van onderzoeken die zijn ingesteld naar aanleiding van een melding van een overheidsorgaan.

Autorisatiebevoegde reisdocumenten
De autorisatiebevoegde reisdocumenten is aangesteld voor de uitvoering van de taken die voor een autorisatiebevoegde RAAS en Aanvraagstation voortvloeien uit de PUN. De autorisatiebevoegde reisdocumenten is rechtstreeks verantwoording schuldig aan de burgemeester zonder tussenkomst van de gegevenseigenaar.

De autorisatiebevoegde reisdocumenten heeft de volgende taken:
- het dagelijks (laten) controleren of de gegevens op de back-up tapes goed zijn weggeschreven, door het controleren van de logbestanden;
- het indien nodig afhandelen van systeemsignalen;
- het dagelijks (laten) opstarten van de aanvraagstations;
- het na gebruik onmiddellijk (laten) opslaan van de identificatie-, authenticatie- (MVA) en opstartkaarten in de kluis in de kluisruimte;
- het onderhouden van contact met de leverancier van de systemen;
- het bekend maken van en toelichting geven over nieuwe of gewijzigde procedures binnen het RAAS of het rijbewijssysteem, in de richting van de betrokken medewerkers;
- het toekennen, wijzigen en intrekken van autorisaties na overleg met de teammanager Burgerzaken en de beveiligingsfunctionaris;
- het bijhouden van een registratie van uitgereikte autorisaties en het afleggen van verantwoording hierover;
- het aan de leverancier en/of RvIG en/of de burgemeester melden van diefstal, verlies of onzorgvuldig gebruik van identificatie-, authenticatie- (MVA) en opstartkaarten;
- het bijhouden van de registratie van ontvangen opstart identificatie-, authenticatie- (MVA) en opstartkaarten;
- het aan de leverancier melden van een defecte of verloren identificatie-, authenticatie- (MVA) en opstartkaarten;
- het opsturen van defecte identificatie-, authenticatie- (MVA) en opstartkaarten naar de leverancier;
- het op juiste wijze laten archiveren van brondocumenten;
- het periodiek uitvoeren van controles op het gebied van autorisaties, functioneel gebruik en correcte verslaglegging hiervan;
- het in ontvangst nemen van Identificatiekaarten en daarop betrekking hebbende codes

Ontvangstbevoegde waardedocumenten
De ontvangstbevoegde waardedocumenten is de medewerker die aangewezen is om een zending in ontvangst te nemen (artikel 81 PUN 2001). Er zijn minimaal drie medewerkers aangewezen om zendingen van reisdocumenten en foto- en handtekeningformulieren in ontvangst te nemen.

4. Passende technische en organisatorische maatregelen
Waardedocumenten
Op grond van de Paspoortwet en daaruit voortvloeiend art. 90 PUN en art. 124 t/m 128 RR is de burgemeester of gezaghebber bevoegd om ten aanzien van de inrichting, werking en beveiliging van de reisdocumentenmodule passende technische en organisatorische maatregelen ter beveiliging van de opgenomen gegevens te treffen.

Deze te treffen maatregelen worden in de procedures behorende bij dit informatiebeveiligingsplan verder uitgewerkt (voor zover deze niet direct voortvloeien uit het GIBB in concrete voorschriften. Artikel 93 lid 1 PUN vereist daartoe organisatorische maatregelen.

BRP
Op grond van artikel 1.11 van de Wet BRP en artikel 6 Besluit BRP is het college van B&W verantwoordelijk om ten aanzien van de gemeentelijke voorziening passende technische en organisatorische maatregelen te treffen ter beveiliging van de in de basisregistratie opgenomen gegevens.

Specifiek gaat het om:
- maatregelen gericht op personen die werkzaam zijn voor de verantwoordelijke voor de verwerking van gegevens in de basisregistratie;
- maatregelen gericht op de toegang tot gebouwen en ruimten waar in de basisregistratie opgenomen gegevens aanwezig zijn;
- maatregelen gericht op een deugdelijke werking en beveiliging van de apparatuur en programmatuur;
- maatregelen voor het geval de geheimhouding of integriteit van in de basisregistratie opgenomen gegevens is geschaad;
- maatregelen bij calamiteiten;
- bewustwording.

Beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid
Welk niveau van technische en organisatorische maatregelen passend is, wordt bepaald door de (data)classificatie waarin persoonsgegevens worden ingedeeld en de context waarbinnen de persoonsgegevens worden verwerkt. Hierbij wordt aangesloten bij het GIBB.

Een passend beveiligingsniveau
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 gedefinieerde (data)classificatie en gerelateerde risico's.

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.
- De kosten van de te treffen maatregelen.

Kwaliteitsaspecten
Het GIBB 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 Purmerend gevolgd moet worden om tot een adequate informatiebeveiliging te komen. Het GIBB vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Het maken en vaststellen van een informatiebeveiligingsbeleid biedt nog geen garantie voor een goede werking van informatiebeveiliging. Hiervoor dienen de uitgangspunten eerst te worden uitgevoerd. Aan de hand van controles op de uitvoering dient het directieteam 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. In de zelfevaluatie wordt niet alleen de kwaliteit van de gegevens maar ook die van processen getoetst en waar nodig aangepast. Deze zelfevaluatie wordt jaarlijks door gemeenten uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken, middels de kwaliteitsmonitor en ENSIA.

Op basis van de dataclassificatie van de persoonsgegevens m.b.t. BRP en waardedocumenten worden de juiste beveiligingsmaatregelen op de volgende onderwerpen genomen:

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. De onderscheiden niveaus zijn: niet nodig; noodzakelijk; belangrijk en essentieel.

Integriteit
De persoonsgegevens moeten in overeenstemming zijn met de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen (juistheid, volledigheid en tijdigheid). De onderscheiden niveaus zijn: niet zeker; beschermd; hoog en absoluut.

Vertrouwelijkheid
De bevoegdheden en de mogelijkheden tot verwerken, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. De onderscheiden niveaus zijn: openbaar; bedrijfsvertrouwelijk; vertrouwelijk en geheim.
Als aanvullende kwaliteitsaspect is de controleerbaarheid van belang.

Controleerbaarheid
Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trails) van groot belang. Controleerbaarheid is de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd en gebruikt.

De gemeente Purmerend hanteert onderstaande normen met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid.

Norm voor beschikbaarheid
De RvIG heeft een informatieblad over BRP en reisdocumenten in het calamiteitenplan gepubliceerd. Hierin wordt gesteld dat het aanvraag- en uitgifteproces van reisdocumenten binnen de gemeentelijke dienstverlening binnen 4 dagen weer operationeel moet zijn. De gemeente houdt dezelfde termijn aan voor rijbewijzen.
Het college van B&W en het directieteam zijn zich ervan bewust dat de bedrijfsvoering geheel stil komt te staan als de informatievoorziening wordt gestaakt en een aantal bedrijf kritische applicaties niet meer functioneren. Dit geldt onder andere en in het bijzonder voor de informatievoorziening vanuit de BRP.
Het college van B&W is zich ervan bewust dat de bedrijfsvoering ernstig kan worden verstoord wanneer de informatievoorziening (gedeeltelijk) uitvalt. 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 niet langer mag duren dan 48 uur. Er dienen adequate voorzieningen te zijn getroffen om ook in geval van calamiteiten binnen maximaal 48 uur de dienstverlening aan de burger en de bestuursorganen te hervatten.
Het functioneren van de BRP en de rijbewijzen- en reisdocumentenadministratie is cruciaal tijdens de openingstijden voor het publiek. De gemeente hanteert een beschikbaarheidspercentage van ≥99% tijdens de openingstijden.
Indien een calamiteit zich voordoet die impact heeft op bedrijfsprocessen/informatievoorziening, kan Team Burgerzaken uitwijken naar een uitwijklocatie. Hiervoor is een uitwijkplan aanwezig.

Norm voor integriteit
De technische en organisatorische inrichting van de gemeentelijke informatiesystemen zijn zodanig van aard en opzet, dat de gegevens daarbinnen volledig, juist, en actueel zijn. De verantwoordelijke personen en teams binnen de gemeentelijke organisatie treffen de benodigde maatregelen om dit zeker te stellen. Het is niet te voorkomen dat gegevens fouten bevatten. Een BRP-bestand zonder fouten is een geweldig streven, maar niet realistisch als concrete eis. Als kwaliteitsnorm voor de kwaliteit van de BRP-gegevens hanteert de gemeente de in de Kwaliteitsmonitor BRP genoemde ondergrens.
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.
Als kwaliteitsnorm bij het bepalen van de kwaliteit van de BRP-gegevens hanteert de gemeente de wettelijk bepaalde normen zoals deze vastliggen in het de Kwaliteitsmonitor (KWM) van de RvIG, waarbij er onderscheid wordt gemaakt tussen 6 klassen.
De RvIG controleert maandelijks de persoonslijsten in de BRP met de Bestandscontrolemodule (BCM). Deze controleert: de structuur van de persoonslijsten, of de ingevulde waarden toegestaan zijn, of de inhoud voldoet aan de voorschriften uit het Logisch Ontwerp (LO).

De resultaten worden maandelijks via de KWM aan gemeenten gerapporteerd. In de onderstaande tabel zijn de door de RvIG vastgestelde normen voor het volledige bestand opgenomen.

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. Administratie	99,4%

Gemeenten voeren jaarlijks een inhoudelijke controle uit op een deel van hun persoonslijsten op basis van brondocumenten. De door de RvIG geselecteerde persoonslijsten worden opgenomen in de KWM. Voor deze bestanden gelden onderstaande normen.

1. Algemene gegevens (Burgerlijke Staat)	A. Persoon en Overlijden	98,0%
	B. Adres	98,0%
	C. Relaties	97,0%
2.Algemene gegevens (overig)	D. Identificatienummers en nationaliteit	96,0%
	E. Overig Algemeen	96,0%
3. Administratieve gegevens	F. Administratie	95,0%
4. Brondocument	G. Niet aanwezig	95,0%

Zodra een binnengemeentelijke afnemer twijfel heeft over de juistheid van een authentiek gegeven dat hij verstrekt heeft gekregen uit de basisregistratie personen, doet hij mededeling aan de gegevenseigenaar. In dat geval wordt er een onderzoek gestart en dossier gevormd. Een eventueel verzoek tot wijziging wordt conform de Algemene wet bestuursrecht (Awb) afgehandeld.

Indien de gegevens in de BRP niet correct zijn (onjuist en/of onvolledig) kan een burger een correctieverzoek indienen bij de gemeente.

Norm voor vertrouwelijkheid
Uitsluitend bevoegde personen in dienst van of werkzaam voor de gemeente Purmerend hebben toegang tot de gegevens en kunnen bij de uitvoer van hun taken, gebruik maken van de in de voor hen relevante registraties opgenomen gegevens. De toegang tot persoonsgegevens door een bevoegd persoon moet worden afgeleid van diens taak, dit ter beoordeling van de gegevenseigenaar, op aangeven van de direct leidinggevende van deze persoon. Team Burgerzaken gebruikt de GABA-autorisatiematrix van de RvIG voor het verstrekken van de juiste autorisaties aan medewerkers. Toegang tot de gebouwen en ruimtes waar de informatie wordt verwerkt, zoals balies, backoffice en de serverruimtes op verschillende locaties wordt verkregen op basis van de taak, dit ter beoordeling van de gegevenseigenaar.

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

Alle medewerkers Burgerzaken (zowel intern als extern) dienen een Verklaring Omtrent Gedrag (VOG) te hebben overlegd. Alle medewerkers binnen de gemeente Purmerend tekenen een integriteitsverklaring zoals beschreven in het Personeelshandboek onder hoofdstuk Integriteit en privacy. Indien geheimhouding wordt geschaad, wordt in eerste instantie de integriteitcoördinator door de teammanager Burgerzaken ingeschakeld om de juiste stappen te bepalen.

Norm voor controleerbaarheid
Mutaties van persoonsgegevens in de BRP kunnen gevolgen hebben die tot ver buiten het domein van de gemeente reiken. Toelating tot Nederland is bijvoorbeeld mede afhankelijk van de nationaliteit van de aanvrager. Hoogte en duur van uitkeringen zijn veelal afhankelijk van leeftijd en de burgerlijke staat. Dat betekent niet alleen dat de kwaliteit van de geregistreerde gegevens hoog dient te zijn, maar lettend op mogelijke belangenverstrengeling dient er ook gecontroleerd te kunnen worden wie welke mutatie heeft uitgevoerd.
De gemeente Purmerend kent als norm dat 99% van alle mutaties van persoonsgegevens herleidbaar moet zijn naar de individuele persoon die daarvoor verantwoordelijk was.

5. Bewustwording
Een gemeente kan nog zo veel technische maatregelen nemen, maar als medewerkers er niet naar handelen hebben deze maatregelen uiteindelijk aanzienlijk minder effect. Daarom wordt er vanuit het GIBB structureel aandacht gegeven aan de bewustwording, kennisontwikkeling, kennisdeling en kennisvermeerdering op het vlak van informatiebeveiliging en privacy in het algemeen.

Gezien het niveau van vertrouwelijkheid van de informatie welke binnen de BRP en waardedocumenten wordt verwerkt, is het van belang dat hier extra aandacht aan wordt gegeven.
Medewerkers die zich niet houden aan de gedragsregels kunnen te maken krijgen met disciplinaire maatregelen die van toepassing zijn op het personeel.

Het is de taak van de teammanager Burgerzaken (gegevenseigenaar) het onderwerp informatiebeveiliging BRP en waardedocumenten periodiek onder de aandacht te brengen bij het personeel en dit vast te leggen. Zo worden de medewerkers die de BRP en BRP-V raadplegen en/of muteren en medewerkers betrokken in het proces van waardedocumenten minimaal twee maal per jaar actief gewezen op het veilig werken.

Nieuwe medewerkers
Alle medewerkers die werkzaamheden verrichten bij Burgerzaken volgen een inwerkplan, waarin onder meer verplichte opleidingen binnen het vakgebied en het veilig omgaan met gegevens zijn opgenomen. Alle medewerkers die de BRP en/of BRP-V raadplegen tekenen hiertoe de 'verklaring gebruik Basisregistratie personen (BRP) en BRP-V' (zie bijlage 1) alvorens de autorisatie wordt verstrekt.

6. Thuiswerken

Gegevens uit de BRP en de BRP-V zijn vertrouwelijk en kwetsbaar, daarom moet de beschikbaarheid, integriteit en vertrouwelijkheid altijd gewaarborgd zijn. De informatiebeveiliging van de BRP-gegevens moet ook extern (buiten het gemeentehuis) gewaarborgd blijven.
Medewerkers die voor hun functie toegang nodig hebben tot de BRP en BRP-V, kunnen werken vanuit huis. Thuiswerken met de BRP en BRP-V gebeurt alleen met toestemming van de werkgever.
De huidige ICT-infrastructuur en beveiligingskaders bieden mogelijkheden om dit op een veilige manier te faciliteren. Om de continuïteit van de dienstverlening te waarborgen.

Thuiswerken wordt mogelijk gemaakt omdat dit bijdraagt aan:
- Continuïteit en efficiëntie van de dienstverlening (ook bij calamiteiten);
- Flexibiliteit in werken.

Bij thuiswerken met toegang tot de BRP en BRP-V is het essentieel dat passende technische en organisatorische maatregelen worden getroffen, zoals vereist onder artikel 32 van de Algemene Verordening Gegevensbescherming (AVG). Deze maatregelen moeten waarborgen dat persoonsgegevens adequaat worden beschermd tegen ongeoorloofde toegang, verlies of andere vormen van onrechtmatige verwerking.

Randvoorwaarden voor thuiswerken met de BRP en BRP-V
Thuiswerken met de BRP en BRP-V is alleen toegestaan onder de volgende voorwaarden:
A. Autorisatie en functiescheiding
- Een verzoek om thuis te werken wordt per email gedaan door de teammanager van de betreffende medewerker en aan de teammanager Burgerzaken.
- Medewerkers mogen alleen thuiswerken met toestemming van de teammanager Burgerzaken op aangeven van de Beveiligingsfunctionaris BRP.
- Functiescheiding wordt gehandhaafd conform de Baseline Informatiebeveiliging Overheid (BIO).

B. Technische beveiliging
- Toegang uitsluitend via gemeentelijk netwerk met beveiligingssoftware die up-to-date is.
- BRP en BRP-V is te allen tijde enkel bereikbaar vanuit de (netwerk)omgeving van de gemeente.
- Gebruik van een multifactor authenticatie wordt verplicht afgedwongen.
- Toegang tot de BRP en BRP-V wordt binnen het netwerk van de gemeente enkel mogelijk gemaakt na invoer van een gebruikersnaam en wachtwoord.

C. Werkplek en fysieke beveiliging
- Medewerkers raadplegen de BRP en BRP-V alleen vanuit huis, dus op een werkplek in de eigen woning.
- De werkplek is zo ingericht dat niemand kan meelezen op het scherm.
- Er wordt enkel digitaal gewerkt; er wordt thuis niets uit de BRP en BRP-V geprint.

D. Bewustzijn
- Medewerkers ondertekenen een aanvullende thuiswerkverklaring m.b.t. gedragsregels over het raadplegen en thuiswerken met de BRP en BRP-V (zie bijlage 2).
- Minimaal twee maal per jaar vind er een bewustwordingsactie onder medewerkers plaats ten aanzien van veilig thuiswerken met de BRP en BRP-V.

7. Functiescheiding waardedocumenten

Reisdocumenten
Functiescheiding is een organisatorisch instrument om te zorgen dat het reisdocumentenproces integer plaatsvindt. Het zorgt ervoor dat er altijd en op zijn minst drie personen betrokken zijn bij het volledige proces van aanvragen tot en met uitreiken. Hiermee wordt voorkomen dat, ook bij externe dwang of chantage, een medewerker in de gelegenheid is om tot frauduleuze handelingen over te gaan.
De PUN schrijft voor dat er altijd minimaal drie personen betrokken zijn bij de verschillende handelingen in de aanvraag, verstrekking en uitgifte van paspoorten en identiteitskaarten:

1. Een medewerker die de identiteit van de aanvrager vaststelt en de aanvraag aanneemt (aanvraag).
2. Een medewerker die de aanvraag mag beoordelen en verzenden naar de producent (verstrekken).

3. Een medewerker die de identiteit van de aanvrager verifieert en het document uitreikt (uitreiken).

De gemeente Purmerend past deze functiescheiding toe door middel van een paraaf van de medewerker op het aanvraag- en uitreikingsformulier. Daarnaast wordt de aanvraag van de ene medewerker, in de backoffice, door een andere medewerker gecontroleerd en doorgestuurd. Door de medewerkers wordt er middels de signalering in de reisdocumentenmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt.

De beheertaken (controleren en inklaren van de documenten) kunnen door één van de drie medewerkers of iemand anders worden uitgevoerd.

Indien door een te geringe personele capaciteit deze functiescheiding niet mogelijk is, kan hier tijdelijk van worden afgeweken. In dat geval zijn er minimaal twee medewerkers betrokken bij het proces. De leidinggevende en/of coördinator van Team Burgerzaken vult hiertoe het C17-formulier van de RvIG in en zorgt dat deze in bewaring wordt genomen. Ten tijde van de controle en zelfevaluatie kan deze worden opgevraagd door het RvIG. Op grond van artikel 93 lid 3 van de PUN worden de volgende punten schriftelijk onderbouwd:

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

Rijbewijzen
Het aan- en uitgifteproces van rijbewijzen komt sinds enkele jaren sterk overeen met dat van reisdocumenten. De artikelen 122 tot en met 130 van het RR 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.

De functiescheiding op dit gebied wordt in de gemeente Purmerend bereikt doordat op het uitreikingsformulier of het aanvraagformulier de paraaf van de medewerker is geplaatst, die over de aanvraag heeft besloten. Door de medewerkers wordt er middels de signalering in de rijbewijsmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt. Daarnaast wordt de aanvraag van de ene medewerker, in de backoffice, door een andere medewerker gecontroleerd en doorgestuurd.

Indien door een te geringe personele capaciteit deze functiescheiding niet mogelijk is, kan hier tijdelijk van worden afgeweken. In dat geval zijn er minimaal 2 medewerkers betrokken bij het proces. De leidinggevende en/of coördinator van Team Burgerzaken stelt hiertoe een schriftelijk besluit op en zorgt dat deze in bewaring wordt genomen. Op grond van artikel 128, lid 3 van het RR worden de volgende voorschriften schriftelijk onderbouwd:
- wat de reden is dat er tijdelijk niet aan de eis van functiescheiding kan worden voldaan;
- binnen welke periode er niet aan de eis van functiescheiding kan worden voldaan;
- wat de namen zijn van de medewerkers, die in deze periode zijn belast met de aanvraag, het beheer en de uitreiking van rijbewijzen.

8. Periodieke zelfevaluatie en onderzoek

Zelfevaluatie Reisdocumenten
Jaarlijks dienen gemeenten een zelfevaluatie voor paspoorten en Nederlandse identiteitskaarten (NIK) en BRP uit te voeren, zoals voorgeschreven door de Paspoortwet en de Wet BRP. De uitkomsten van de zelfevaluaties worden naar de RvIG gezonden door het college van B&W voor wat betreft de BRP, en door de burgemeester voor wat betreft de reisdocumenten.

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 KWM. Met behulp van een persoonlijke log-in kan elke gemeente in het onderdeel ‘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.

Onderzoek BRP
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 KWM aan gemeenten beschikbaar stelt en een vragenlijst binnen ENSIA. Deze vragenlijsten moeten jaarlijks vóór 31 december definitief zijn ingevuld. De managementrapportage die de KWM genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsfunctionaris BRP en waardedocumenten en voorzien van een actieplan van de gemeente) worden aangeboden aan het college. Het bestuursorgaan, het college, ondertekent het bijbehorende uittreksel en stuurt deze vóór 30 april naar de RvIG en Autoriteit Persoonsgegevens (AP). De beveiligingsfunctionaris BRP en rij- en reisdocumenten houdt toezicht op de te ondernemen acties naar aanleiding van de jaarlijkse zelfevaluatie.

Onderzoek waardedocumenten
Jaarlijks dient de gemeente een onderzoek te doen naar de inrichting, werking en beveiliging rondom reisdocumenten. Dit dient de gemeente Purmerend te doen door middel van een zelfevaluatie (art. 94 PUN). Deze controle voert de gemeente uit aan de hand van een digitale vragenlijst waardedocumenten die de RvIG via de KWM aan gemeenten beschikbaar stelt en een vragenlijst binnen ENSIA. Deze vragenlijst moet jaarlijks vóór 31 december definitief zijn ingevuld.
De managementrapportage die de KWM genereert na het definitief invullen van de vragenlijst, moet (eventueel aangevuld met de bevindingen van de beveiligingsfunctionaris BRP en waardedocumenten 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 30 april naar de RvIG. De beveiligingsfunctionaris BRP en rij- en reisdocumenten houdt toezicht op de te ondernemen acties naar aanleiding van de jaarlijkse zelfevaluatie.

9. Vaststelling

Dit informatiebeveiligingsplan treedt in werking na vaststelling door het college en de burgemeester onder gelijktijdige intrekking van:
- het informatiebeveiligingsplan Basisregistratie Personen 2019-2021,
- het informatiebeveiligingsplan Reisdocumenten en Rijbewijzen 2019-2021, en
- de Beheerregeling basisregistratie personen (BRP) Purmerend.

Aldus vastgesteld door burgemeester en wethouders en de burgemeester van gemeente Purmerend,

Datum: 23 juni 2026

burgemeester en wethouders,

de secretaris,
M.H. van der Weit

de burgemeester,
E. van Selm

de burgemeester,
E. van Selm

Bijlage 1 Verklaring gebruik Basisregistratie personen (BRP) en BRP-V

Naam en voornamen	
Domein	
Team	
Functie	
Datum in dienst	

Je hebt toegang gekregen voor het raadplegen van de Basisregistratie personen (BRP). Aan deze toegang zijn regels verbonden. Je bent geautoriseerd voor de BRP en/of voor de landelijke Basisregistratie personen (BRP-V).

De toegang tot de BRP en BRP-V is beveiligd. Om misbruik van de gegevens te voorkomen wordt bijgehouden wie gegevens in de BRP of BRP-V raadpleegt of wijzigt. Er wordt ook bijgehouden van wie je gegevens raadpleegt.

Naast het gestelde in de gedragscode en het privacyreglement willen wij je nog even extra attenderen op de volgende bijzonderheden die voor de BRP en BRP-V gelden, en verklaar jij dat je:

- alleen gegevens uit de BRP of BRP-V opvraagt die nodig zijn voor de uitvoering van je werkzaamheden;
- gegevens van inwoners van Purmerend alleen raadpleegt in de BRP. De BRP-V raadpleeg je alleen voor inwoners van buiten Purmerend;
- geen persoonsgegevens uit de basisregistratie personen verstrekt of ter inzage geeft (niet telefonisch of schriftelijk) aan derden - intern en extern - zonder daartoe strekkend mandaat;
- verplicht bent tot geheimhouding van al datgene wat jou in jouw dienstverband ter kennis komt, tenzij enig wettelijk voorschrift mededeling vordert;
- bekend bent dat ten aanzien van de geheimhouding in de wet is bepaald dat schending van de geheimhoudingsplicht een zogenaamde dringende reden kan betekenen die ontslag op staande voet rechtvaardigt;
- geen andere personen gebruik laat maken van de BRP of BRP-V via jouw computer en/of jouw inloggegevens;
- dat je bij het verlaten van de werkplek alle sessies van applicaties die toegang geven tot de BRP en BRP-V afsluit;
- deze verklaring blijft van kracht, ook na beëindiging van bovengenoemde werkzaamheden.

Om gegevens in de BRP te mogen gebruiken of bekijken, gelden regels. Die staan in de Algemene Verordening Gegevensbescherming (AVG) en de Wet basisregistratie personen (Wet BRP). De Autoriteit persoonsgegevens (AP) ziet toe op de naleving van deze wetten.

Op de website van de Autoriteit Persoonsgegevens staat meer informatie voor gemeenten over AVG-plichten bij de Wet BRP.

Alleen organisaties met een publieke of maatschappelijke taak kunnen gegevens uit de BRP of BRP-V krijgen. De regels daarover staan in de Wet BRP. Deze organisaties krijgen alleen die gegevens die zij nodig hebben. Waarvoor een organisatie persoonsgegevens krijgt, en welke gegevens dat zijn, ligt vast in een autorisatiebesluit.

Persoonsgegevens in de BRP worden voor altijd bewaard. Als een organisatie persoonsgegevens uit de BRP krijgt, wordt de registratie van deze verstrekking 20 jaar bewaard.

Met het ondertekenen van dit document verklaar ik dat ik de inhoud van dit document heb doorgelezen en heb begrepen. Tevens verklaar ik dat ik me aan de gedragsregels zal houden.

Datum	Handtekening

Bijlage 2 Verklaring gebruik Basisregistratie personen (BRP) en BRP-V tijdens thuiswerken

Naam en voornamen	
Domein	
Team	
Functie	
Datum in dienst	

Je hebt toegang gekregen voor het raadplegen van de BRP vanaf je thuiswerkplek. Naast de gebruikelijke regels voor het werken met de BRP gelden daarvoor aanvullende voorwaarden.

De toegang tot de BRP is beveiligd. Om misbruik van de gegevens te voorkomen wordt bijgehouden wie gegevens in de BRP raadpleegt of wijzigt. Er wordt ook bijgehouden van wie je gegevens raadpleegt.

Naast het gestelde in de gedragscode van de gemeente Purmerend en het privacybeleid van de gemeente Purmerend willen wij je nog even extra attenderen op de volgende bijzonderheden die voor het thuiswerken met de BRP en BRP-V gelden, en verklaar jij dat je:

- gebruik van de BRP en BRP-V buiten het kantoor is alleen toegestaan op een werkplek in de eigen woning en uitsluitend vanuit de voorzieningen die de gemeente ondersteund;
- toegang uitsluitend via gemeentelijk netwerk met beveiligingssoftware die up-to-date is;
- BRP en BRP-V is te allen tijde uitsluitend bereikbaar vanuit de (netwerk)omgeving van de gemeente;
- gebruik van een twee-factor authenticatie wordt verplicht afgedwongen;
- toegang tot de BRP en BRP-V wordt binnen het netwerk van de gemeente enkel mogelijk gemaakt na invoer van een gebruikersnaam en wachtwoord. Je deelt je gebruikersnaam en wachtwoord met niemand.

Werkplek en fysieke beveiliging

- medewerkers raadplegen de BRP en BRP-V alleen vanuit huis, dus op een werkplek in de eigen woning.
- de werkplek is zo ingericht dat niemand kan meelezen op het scherm.
- als de werkplek wordt verlaten en er zijn andere mensen aanwezig in de woning, wordt de burgerzakenapplicatie afgesloten.
- deze verklaring blijft van kracht, ook na beëindiging van bovengenoemde werkzaamheden.

Om gegevens in de BRP en of BRP-V te mogen gebruiken of bekijken, gelden regels. Die staan in de Algemene Verordening Gegevensbescherming (AVG) en de Wet basisregistratie personen (Wet BRP). De Autoriteit persoonsgegevens (AP) ziet toe op de naleving van deze wetten.

Op de website van de Autoriteit Persoonsgegevens staat meer informatie voor gemeenten over AVG-plichten bij de Wet BRP.

Persoonsgegevens in de BRP worden voor altijd bewaard. Als een organisatie persoonsgegevens uit de BRP krijgt, wordt de registratie van deze verstrekking 20 jaar bewaard.

Met het ondertekenen van dit document verklaar ik dat ik de inhoud van dit document heb doorgelezen en heb begrepen. Tevens verklaar ik dat ik me aan de gedragsregels zal houden.

Datum	Handtekening