Rijndijk 235
2394 CD Hazerswoude
Tel. (071) 3416911
Email noordbeek@noordbeek.com

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directoraat-generaal Overheidsorganisatie (DGOO)
Directie Informatiesamenleving en Overheid (I&O)

# Rapport van Bevindingen aangaande een

# Doorlichting digitale veiligheid

# Basisregistratie Personen (BRP)

Definitieve versie: 1.00

| | |
|---|---|
| Opdrachtgever | Ministerie BZK, DGOO, I&O, Afd. Identiteit |
| Auteur | R. Paans Noordbeek |
| | S.D. Kubacki |
| | J. Winkel |
| Rapportnummer | KPNBRP9-1 |
| Classificatie | Openbaar |
| Status | Definitief |
| Datum | 18 oktober 2019 |
| Bestandsnaam | Rapport Noordbeek Doorlichting Veiligheid BRP - Openbaar |
| KvK nummer | Rijnland 33265070 |
| BTW nummer | NL8203.45.180.B01 |

**Colofon**

| | |
|---|---|
| Opdrachtgever | Directie Informatiesamenleving en Overheid (I&O), Afd. Identiteit<br>Directoraat-generaal Overheidsorganisatie (DGOO)<br>Ministerie van Binnenlandse Zaken en Koninkrijksrelaties |
| Opdrachtnemer | E. van Essen<br>Account Director Centrale Overheid<br>KPN |
| Onderaannemer KPN<br>Contactpersoon | Prof. dr.ir. R. Paans RE<br>Directeur Noordbeek B.V. |
| Auteurs | R. Paans<br>S.D. Kubacki<br>J. Winkel |
| Kwaliteitscontrole | M.H.N. de Roo<br>W.H. Mulder |

**Inhoud**

# 1. Inleiding

Het ministerie van Binnenlandse zaken en Koninkrijksrelaties (BZK) heeft KPN en haar onderaannemer Noordbeek opdracht gegeven een doorlichting digitale veiligheid Basisregistratie Personen (BRP) uit te voeren.

## *1.1. De achtergrond van de opdracht*

In het Regeerakkoord (bijlage bij Kamerstuk 34 700, nr. 34) is opgenomen dat gegevens van burgers in basisadministraties en andere privacygevoelige informatie altijd versleuteld worden opgeslagen. In de Kamerbrief 'Verhogen informatiebeveiliging' van 16 oktober 2018 wordt hierover de volgende aanpak met de Kamer gedeeld: '*Zodoende wordt gestart met een onderzoek naar de wijze waarop de huidige veiligheidsmaatregelen afdoende bescherming bieden tegen mogelijke beveiligingsrisico's. Uitgangspunt daarbij is het beschermen van privacygevoelige informatie. Hieruit kan volgen dat registraties of onderdelen van registratiesystemen die nu niet zijn versleuteld dat voortaan wel moeten worden*.' De BRP is de eerste basisregistratie waarvoor dit onderzoek is uitgevoerd.

De BRP bevat de persoonsgegevens van mensen met een band met de Nederlandse overheid en is daarmee de basis voor het identiteitsstelsel. Met behulp van de gegevens in deze registratie kunnen rechten en plichten worden gekoppeld aan personen. De gegevens worden bijgehouden door gemeenten. Afnemers van deze informatie zijn diverse organisaties met een publieke taak, zoals de Belastingdienst en UWV.

De BRP is een systeem dat goed moet worden beveiligd omdat de informatie uit de BRP correct moet zijn, maar ook omdat de gegevens niet openbaar zijn. De behoefte tot inzage, manipulatie, verwijderen of toevoegen van gegevens is aanwezig. Identiteitsfraude ligt aan de basis van misdaad en terreur. Voor de BRP zijn reeds diverse veiligheidsmaatregelen genomen. Deze veiligheidsmaatregelen zijn onder andere gebaseerd op de Baseline Informatiebeveiliging Rijk / Technisch Normenkader (BIR/TNK), ISO 27001 en ISO 27002. De mogelijkheden die kwaadwillenden hebben en de te beschermen belangen zijn echter aan het verschuiven. Hierdoor ontstaat de behoefte voor een doorlichting van de actuele veiligheid van de BRP.

## *1.2. De aard en het doel van de opdracht*

De opdracht is een veiligheidsonderzoek naar de ICT-componenten van de BRP. Hoewel al diverse maatregelen zijn genomen bestaat de behoefte deze te doorlichten tegen (mogelijk) nieuwe risico's. Het kabinet hecht veel belang aan het veilig houden van privacygevoelige informatie.

Het doel van de opdracht is inzichtelijk te krijgen waar de data uit de BRP zich bevindt, hoe deze is afgeschermd, of er nieuwe risico's zijn, welke risico's onvoldoende zijn afgedekt en welke bijbehorende maatregelen kunnen worden genomen. Het gaat daarbij om ongeautoriseerde toegang tot data, de manipulatie van data en inzicht in data. Bij de resultaten dient ook te worden ingegaan op de haalbaarheid en proportionaliteit van de aangedragen maatregelen.

### *1.3. Het doel*

Het doel van de opdracht is een overzicht verkrijgen van de risico's voor de BRP, met bijgevoegd een inschatting van hoe hoog de dreiging wordt geschat. Bij elk risico is een overzicht van bijpassende maatregelen gegeven, inclusief een kosten-batenanalyse.

Een gewenst bijproduct is een geprioriteerde lijst met actoren die een potentieel risico voor de BRP vormen en wat de te verwachten modus operandi is.

### *1.4. De doelgroep voor het rapport*

De eindgebruikers van de opgeleverde producten zijn de Rijksdienst voor Identiteitsgegevens (RvIG) en het ministerie van BZK.

### *1.5. Scope*

Het onderzoek is gericht op de digitale processen en hoe ongeautoriseerde toegang tot de data kan worden voorkomen. De BRP is een groot systeem, met diverse centrale en decentrale voorzieningen. Niet al deze componenten kunnen bij het onderzoek worden doorgelicht. Wel zijn de kaders en afspraken die zijn gemaakt met gemeenten en afnemers doorgelicht.

Het onderzoek betreft de situatie op 30 april 2019.

De volgende objecten van onderzoek zijn onderkend:
- GBA-netwerk met het X.400 'simple Protocol data' (sPd)-protocol;
- GBA-Verstrekkingen (GBA-V);
- Registratie Niet-Ingezetenen (RNI);
- Terugmeldvoorziening (TMV);
- Verstrekkingsvoorziening Daft (voor synchroniteit);
- De inhoud van de centrale (persoons)gegevens.

De opdrachtgever heeft bepaald welke componenten buiten de scope vallen van dit onderzoek. Dit zijn onder andere:
- Beheervoorziening BSN (BV-BSN);
- Gemeentelijke afnemers en leveranciers, met hun lokale GBA-databases;
- Niet gemeentelijke afnemers, met hun verrijkte persoonsgegevens;
- IND als afnemer en leverancier, met het systeem Indigo voor het behandelen van verblijfsaanvragen en naturalisaties;
- Het Caribisch gebied met de PIVA-GBA-Koppeling (PGK), PIVA-Verstrekkingen (PIVA-V) en de zes PIVA-databases in Caribisch Nederland, Aruba, Curaçao en Sint Maarten.

Voor de uitvoering van de werkzaamheden en rapportage volgt Noordbeek de Code of Ethics en richtlijnen van de beroepsorganisatie voor IT-auditors, de Nederlandse Orde van Register EDP Auditors (NOREA).

### *1.6. Beperkingen*

Alle in dit rapport opgenomen informatie over de BRP en cyberdreigingen is verkregen via publiekelijk toegankelijke bronnen. Voor de kwetsbaarhedenanalyse is gebruik gemaakt van de professionele ervaring van de onderzoekers en collega IT-auditors bij het uitvoeren van veel IT-audits binnen en buiten de overheid gedurende de afgelopen 25 jaar.

Via interviews en deskresearch zijn de opzet en het bestaan van de IT-beheersingsmaatregelen geïnventariseerd.

Het onderzoek en de rapportage is, gegeven de opdracht, toegespitst op de IT-gerelateerde elementen die van belang zijn voor de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens in de BRP en voor het inschatten van de risico's voor de digitale veiligheid van de BRP.

# 2. Conclusie en adviezen

## *2.1. Conclusie over de waarde van en risico's voor de BRP-gegevens*

De BRP is benoemd als een basisregistratie, maar is vanuit technisch oogpunt geen entiteit. Het is een verzameling van honderden zelfstandige systemen, ieder met hun eigen gegevensverzamelingen. Deze systemen zijn ingericht en worden beheerd door vele organisaties, die ieder hun eigen beheers- en beveiligingsmaatregelen hebben getroffen.

### *2.1.1. Inhoud van de BRP en verantwoordelijkheden*

Het centrale gedeelte van BRP wordt beheerd door de Rijksdienst voor Identiteitsgegevens (RvIG). De decentrale leveranciers van de persoonsgegevens zijn de gemeenten via hun Gemeentelijke Basis Administratie (GBA) systemen. Bij iedere gemeente is het college van burgemeester en wethouders de verwerkingsverantwoordelijke, conform de AVG. In het centrale gedeelte wordt alleen een kopie bijgehouden van een deel van de lokale gemeentelijke GBA-gegevens, namelijk in het systeem GBA-Verstrekkingen (GBA-V). De kopie in GBA-V omvat de persoonslijst per ingezetene (PL), dat een beperkt uittreksel is van de bij de gemeente beschikbare persoonsgegevens, en de verwijsgegevens. Tevens zijn het GBA-netwerk en de Registratie Niet Ingezetenen (RNI) centraal ingericht.

Een gemeente is naast leverancier van persoonsgegevens tevens afnemer van GBA-V, evenals de Immigratie en Naturalisatie Dienst (IND). Daarnaast zijn er honderden afnemers van GBA-V in het kader van belastingen, toeslagen, sociale zekerheid, gezondheidszorg, kinderbescherming, pensioenen, verzekeringen, openbare orde en veiligheid etc. Al deze afnemers ontvangen geselecteerde persoonsgegevens vanuit GBA-V en verrijken die in hun eigen systemen, gericht op hun zakelijke doeleinden. Iedere afnemende organisatie is een zelfstandige verwerkingsverantwoordelijke voor hun verrijkte persoonsgegevens, conform de AVG.

### *2.1.2. Waarde van de BRP-gegevens*

De persoonsgegevens in de BRP hebben een substantiële waarde voor niet-statelijke en statelijke dreigende actoren, onder andere in het kader van identiteitsfraude, onrechtmatig verkrijgen van adressen, ongewenste buitenlandse inmenging in diaspora, aantasting van democratische processen en instituten, benadeling van bepaalde groepen van minderheden etc.

Tevens kunnen niet-statelijke en statelijke dreigende actoren mogelijkheden zoeken om persoonsgegevens in de BRP te kunnen muteren, onder andere in het kader van het verschaffen van een nieuwe identiteit aan terugkerende terroristen, mensenhandel, mensensmokkel, fraude met sociale zekerheid (onder andere via adresfraude), intimidatie in diaspora etc.

### *2.1.3. De uitgevoerde risicoanalyses voor de BRP*

Binnen dit onderzoek is een aantal risico's voor de BRP in kaart gebracht, met een inschatting van de ernst van de dreiging. Op basis van publiekelijk toegankelijke literatuur zijn dreigingsscenario's uitgewerkt, gericht op de vertrouwelijkheid, de integriteit en de beschikbaarheid van de persoonsgegevens in de BRP.

Uit de scenarioanalyse volgt dat de pure gegevens uit de BRP, eventueel aangevuld met de verrijkte gegevensverzamelingen, een substantiële waarde hebben voor kwaadwillende actoren die daar misbruik van willen maken. Deze scenario's betreffen:

- Risico's voor partners met gelijk geslacht, die bij onthulling van hun geaardheid in (levens)gevaar kunnen komen in bepaalde landen;
- Risico's voor critici op buitenlandse dictatoriale regimes, waarbij die regimes spionnen kunnen werven of critici kunnen intimideren of afpersen;
- Risico's voor buitenlandse inmenging;
- Misbruik van identiteitsgegevens en adressen.

Onrechtmatige mutaties op gegevens in de BRP, of het weglaten van bepaalde mutaties, kunnen leiden tot onder andere:

- Adresfraude.

De werking van de BRP kan worden gesaboteerd, waardoor het vertrouwen van de ingezetenen in de overheid kan afnemen, onder andere door:

- Besmetting met ransomware of wiperware, waardoor (delen van) de BRP niet meer toegankelijk zijn;
- Ongeautoriseerde invoer van corrupte persoonsgegevens, waardoor de authenticiteit van de gegevens in de basisregistratie niet meer is geborgd.

De wijze waarop kwaadwillende actoren te werk gaan is uitgewerkt in de volgende scenario's:

- Diefstal van een fysiek medium;
- Onbetrouwbare of afgeperste medewerker;
- Digitale inbraken via vele modus operandi;
- Uitlekken van wachtwoorden;
- Kraken van wachtwoorden.

### *2.1.4. Risicoinschatting voor de BRP-gegevens*

Wij schatten de mate van risico hoog in voor de gemeentelijke GBA-systemen, aangezien persoonsgegevens in die systemen relatief eenvoudig toegankelijk zijn voor dreigende actoren en door hen kunnen worden gemanipuleerd.

Wij zien een substantieel risico voor de vertrouwelijkheid van de persoonsgegevens bij de verrijkte gegevensverzamelingen bij de vele afnemers. De waarde van verrijkte gegevensverzamelingen is voor dreigende actoren hoger dan de waarde van pure GBA-gegevens, namelijk de persoonslijsten en verwijzingen, aangezien verrijkte gegevens doelgerichter kunnen worden misbruikt.

Het risico voor vertrouwelijkheid bij de centrale GBA-V zien wij als bestaand maar lager, aangezien in GBA-V slechts een deel van de persoonsgegevens is gekopieerd, namelijk alleen de persoonslijsten en verwijsgegevens. Niettemin zijn er dreigingsscenario's voor het ontvreemden en misbruiken van de pure GBA-gegevens vanuit GBA-V.

Wij schatten het risico voor de integriteit van de persoonsgegevens in GBA-V in als hoog, aangezien een onrechtmatige mutatie in GBA-V rechtstreeks wordt doorgekopieerd naar de relevante afnemers.

Wij schatten het risico voor de beschikbaarheid van GBA-V en de aangesloten systemen als hoog in het geval van een aanval met ransomware of wiperware. Het is mogelijk dat de processen rondom burgerzaken dan langdurig verstoord kunnen raken.

### *2.1.5. Ineffectiviteit van het huidige stelsel van maatregelen*

Het gehele stelsel van maatregelen voor informatiebeveiliging en privacybescherming is historisch gegroeid, gedistribueerd over vele honderden verwerkingsverantwoordelijken en niet ingericht om in afdoende mate weerstand te bieden tegen de actuele dreigingen in 2019. Zwakke punten bij gemeenten en afnemers zijn over het algemeen een te brede ontsluiting van gegevens en functionaliteiten, historisch gegroeide informatiestromen waarbinnen verschillende soorten gegevens worden vermengd, ineffectief autorisatiebeheer voor gebruikers en lokale beheerders, onvoldoende vastlegging en toezicht, uitbesteding met beperkte privacy-waarborgen en onvoldoende aansturing voor informatiebeveiliging en privacybescherming.

| |
|---|
| Op dit moment is het gehele stelsel van maatregelen voor informatiebeveiliging en privacybescherming niet in staat om de persoonsgegevens van de BRP adequaat te beschermen tegen ontvreemding of onrechtmatige mutatie. |

De kern van het beveiligingsprobleem ligt in de opzet en structuur van de BRP, zoals die is voorgeschreven in de Wet BRP. Hierbij is ieder college van burgemeester en wethouders een zelfstandig beheerder en leverancier van persoonsgegevens, en alle afnemers kunnen zelfstandig over hun deel van de persoonsgegevens beschikken. In deze opzet is niemand daadwerkelijk eindverantwoordelijk voor het geheel aan persoonsgegevens, niemand kent de specifieke risico’s voor de vele informatiestromen en niemand heeft de bevoegdheid om adequate maatregelen treffen voor een integrale beveiliging. Hiermee wordt niet gezegd dat gemeenten en afnemers onzorgvuldig zijn, aangezien er lokaal veel belangrijke maatregelen wel zijn gerealiseerd, maar een ketting is zo sterk als haar zwakste schakel.

### *2.2. Conclusie over de ineffectiviteit van het versleutelen van GBA-V*

Het voorstel dat gegevens van burgers in basisadministraties en andere privacygevoelige informatie altijd versleuteld worden opgeslagen, zoals vermeld in het Regeerakkoord (bijlage bij Kamerstuk 34 700, nr. 34) en de Kamerbrief 'Verhogen informatiebeveiliging' van 16 oktober 2018, mitigeert naar onze mening slechts één bestaand beveiligingsrisico voor de BRP. Dat is het risico voor het ontvreemden van een fysieke computerschijf met een enkelvoudige BRP-gegevensverzameling vanuit een rack in een datacenter, of het ontvreemden van een kopie of back-up van zo een gegevensverzameling. Voor alle andere dreigingen heeft het versleutelen van een gegevensbestand geen toegevoegde waarde, aangezien zowel de leveranciers als de afnemers van de persoonsgegevens deze gegevens onversleuteld moeten kunnen verwerken.

#### *2.2.1. Risico's liggen vooral buiten de centrale database GBA-V*

Gemeenten, pensioenfondsen, verzekeraars, de Belastingdienst, UWV, SVB en vele andere partijen zijn afnemers van de BRP. In totaal zijn dit zo een 1.200 instanties. Zij beschikken over veel meer persoonsgegevens dan in de BRP staan, en verwerken die binnen hun operationele processen. Deze persoonsgegevens staan in vele databases, zijn onderdeel van vele informatiestromen binnen en tussen deze partijen, en worden verwerkt binnen vele verschillende informatiesystemen, zowel lokaal bij die instanties als op afstand via bijvoorbeeld Software as a Service (SaaS) of Application Service Providers (ASP's) bij leveranciers.

Gemeenten zijn tevens de leveranciers van de persoonsgegevens die worden opgeslagen in de centrale database GBA-V. De met GBA-V uit te wisselen gegevens vormen echter een zeer beperkte deelverzameling van de bij de instanties zelf beschikbare persoonsgegevens. De persoonsgegevens in GBA-V betreffen vooral naam, adres, woonplaats, BSN, nationaliteit, geboortedatum en directe familierelaties. Deze gegevens hebben een beperkte waarde voor dreigende actoren. Zij kunnen worden misbruikt, maar met weinig profijt.

Vanuit het oogpunt van misbruik zijn de persoonsgegevens bij de 1.200 aangesloten instanties waardevoller dan de persoonsgegevens in GBA-V. Daar zijn veel gegevens over de persoonlijke levenssfeer, het persoonlijk gedrag van mensen en hun voorkeuren, hun inkomen, hun bezittingen en vermogen, en andere zaken die hen mogelijk chantabel maken of hen interessant maken voor criminelen. Inbreken bij deze instanties heeft voor een dreigende actor meer profijt dan inbreken in GBA-V.

De dreigingen voor de vertrouwelijkheid van de persoonsgegevens liggen vooral buiten de centrale database GBA-V. Deze dreigingen zijn niet los te zien van de aangesloten instanties en hun IT-leveranciers.

Dreigingen voor de integriteit van de persoonsgegevens liggen vooral bij gemeenten als de leveranciers van die gegevens. De kans dat een dreigende actor persoonsgegevens manipuleert bij een gemeente is substantieel hoger dan de kans dat die dreigende actor ongemerkt rechtstreeks iets in GBA-V weet te veranderen.

### *2.2.2. Technische aspecten van het versleutelen van GBA-V*

Versleutelen van persoonsgegevens in en rondom de BRP kan op verschillende manieren.

Als eerste mogelijkheid kan men de GBA-V database zelf versleutelen, waarbij de gegevens worden ontsleuteld alvorens die naar de afnemers worden gestuurd. Dit beschermt tegen diefstal van de fysieke schijf of tegen het illegaal kopiëren van de centrale database GBA-V. Maar het beschermt niet tegen alle vormen van opvragingen door de aangesloten instanties en beschermt ook niet tegen frauduleuze mutaties die door dreigende actoren via gemeenten worden aangeleverd.

Momenteel is het netwerk tussen GBA-V en de afnemers al versleuteld, waarbij aan de zijde van de ontvanger wordt ontsleuteld. Dit beveiligingsproces is centraal ingericht met certificaten. De ontvanger krijgt het bericht in leesbare tekst.

Als tweede mogelijkheid zou men het centrale systeem en netwerk zo kunnen inrichten dat de afnemers versleutelde persoonsgegevens ontvangen en de gemeenten de persoonsgegevens versleuteld moeten aanbieden. Dit heeft als nadeel dat alle aangesloten partijen moeten beschikken over het versleutelalgoritme en passende sleutels. Gezien het grote aantal instanties, die niet allemaal gedegen zijn beveiligd, heeft dit als nadeel dat het algoritme en de sleutel in handen kunnen komen van dreigende actoren. Tevens geldt het nadeel dat alle andere persoonsgegevens binnen de instantie, die waardevoller zijn voor een dreigende actor, nog steeds in leesbare tekst lokaal aanwezig zijn.

Als derde mogelijkheid zou men alle aangesloten instanties kunnen verplichten alle lokale persoonsgegevens op een afdoende wijze te versleutelen. Dit is echter per instantie een kostbare operatie, aangezien die gegevens worden gebruikt in lokale databases, systemen en informatiestromen, en op velerlei wijze lokaal worden opgslagen. Daarnaast mist RvIG de bevoegdheid zo een drastische maatregele op te leggen aan de instanties.

### *2.2.3. Randvoorwaarde: toegankelijkheid voor rechtmatige gebruikers*

Een belangrijke randvoorwaarde is dat de vele duizenden medewerkers binnen de werkprocessen van de aangesloten instanties moeten werken met de persoonsgegevens. Dit houdt in dat zij de gegevens ongehinderd moeten kunnen raadplegen en muteren, conform hun bevoegdheden.

Binnen de huidige opzet is het vanuit het GBA-V niet mogelijk om vast te stellen welke transactie en verzoeken vanaf de verschillende partners en aangesloten instanties rechtmatig zijn. Het is onmogelijk voor de GBA-V om te zien of een verzoek wellicht wordt gedaan door een ongautoriseerd persoon die toegang heeft tot credentials van geautoriseerde medewerkers.

Het GBA-V is genoodzaakt er op te vertrouwen dat alles wat de aangesloten partijen doen rechtmatig is. Het GBA-V steunt hierbij op de kwaliteit van het access-management van alle aangesloten partijen. Aangezien vele gebruikers uitgebreide leesrechten hebben, kan een kwaadwillende via een aangesloten partij proberen toegang te verkrijgen tot de gegevens in het GBA-V.

Hierbij is de bescherming zo sterk als de zwakste schakel. Encryptie van GBA-V heeft geen invloed op dit risico. Dit brede gebruik maakt een gedegen wijze van versleutelen vrijwel onmogelijk.

### *2.3. Adviezen*

De standaardadviezen voor het verbeteren van de beveiligingsmaatregelen, zoals het verhogen van de awareness en de Baseline Informatiebeveiliging Overheid (BIO) (of de internationale standaard ISO/IEC 27001:2013) voorschrijven voor de leveranciers en afnemers zijn nodig, maar leiden naar verwachting niet tot een volledige mitigatie van de in dit rapport gesignaleerde risico's.

Dergelijke adviezen zijn te generiek en pakken niet de werkelijke dreigingen aan. Daarvoor is een meer drastische aanpak nodig. Wij adviseren bij de toekomstige ontwikkelingen van het BRP te overwegen af te stappen van de gedistribueerde structuur en over te gaan naar een centrale opslag van de persoonsgegevens die authentiek dienen te zijn.

Daarbij past een centrale organisatie die richtlijnen uitvaardigt voor actuele dreigingen op basis van een actuele informatiepositie, toezicht houdt op mutaties en verstrekkingen, en centrale logging en monitoring inricht, aangevuld met data analytics. Deels is dit een functie voor een centraal Security Operating Center (SOC) gericht op de basisregistratie BRP, die tevens de actuele lokale autorisaties bewaakt, technische kwetsbaarhedenanalyses (vulnerability scans) laat uitvoeren etc.

Om meer inzicht te krijgen in de actuele status van informatiebeveiliging en privacybescherming bij gemeenten kan mogelijk worden aangesloten bij de Eenduidige Normatiek Single Information Audit (ENSIA). Daarbij worden jaarlijks vragen gesteld aan de gemeenten over onder andere awareness, logging en monitoring, anonimisering van testgegevens etc. Een analyse van de antwoorden van de gemeenten kan worden gebruikt om de in dit rapport genoemde risico's te kwantificeren.

### *2.4. Bevindingen*

Wij hebben waargenomen dat de geïnterviewde medewerkers competent en betrokken zijn in het kader van een zorgvuldige beheersing van de IT, maar dat de BRP op het vlak van aantoonbaarheid van de getroffen maatregelen nog enkele onvolkomenheden kent.

De door ons gesignaleerde aandachtspunten zijn:

1. **Gefragmenteerde IT-organisatie en Control**
   RvIG is de verwerkingsverantwoordelijke voor de centrale voorzieningen zoals het GBA-netwerk, GBA-V, RNI etc. De inrichting en het beheer van de infrastructuur is uitbesteed aan de Dienst ICT Uitvoering (DICTU), onderdeel van het ministerie EZK. Het college van burgemeester en wethouders van een gemeente is de verwerkingsverantwoordelijke voor hun gemeentelijk GBA-systeem. De leiding van een afnemende organisatie is de verwerkingsverantwoordelijke voor hun afnemerssysteem.
   Wij constateren dat diverse verantwoordelijkheden en functies zijn voorgeschreven en belegd, maar dat centrale aansturing en centraal toezicht ontbreekt door de gedistribueerde opzet van de BRP. Als de inrichting of beveiliging bij een van de vele betrokken partijen niet op orde is, faalt in feite het gehele stelsel van maatregelen voor informatiebeveiliging en privacybescherming. Een ketting is zo sterk als haar zwakste schakel.
   Wij adviseren bij de toekomstige ontwikkelingen van het BRP te overwegen af te stappen van de gedistribueerde structuur en over te gaan naar een centrale opslag van de persoonsgegevens die authentiek dienen te zijn.

2. **Geen actuele risicobeheersing**
   Volgens de documentatie van de BRP moeten de beveiligingsmaatregelen binnen de verschillende onderdelen van het GBA-systeem met elkaar in evenwicht zijn. De generieke (in)effectiviteit van beveiligingsmaatregelen binnen Nederland wordt beschreven in diverse stukken, zoals in de recente brief van 18 april 2019 van NCTV aan de Tweede Kamer, ‘Tegengaan statelijke dreigingen, kenmerk 2573867’.
   Wij constateren dat momenteel het inzicht in de risico’s van statelijke actoren groeit, maar dat dit inzicht niet is gebruikt voor het verder verbeteren van de beveiligingsmaatregelen voor de BRP. Het concept van het GBA-netwerk stamt uit de tachtiger jaren van de vorige eeuw. Later zijn in beperkte mate beveiligingsmaatregelen zoals certificaten toegevoegd, maar het probleem van gedistribueerde gegevens onder de verantwoordelijkheid van vele partijen is nimmer integraal opgepakt.
   Het risico is dat het historisch ontwikkelde stelsel van beveiligingsmaatregelen voor BRP niet adequaat is voor de meer recente vormen van dreigingen. Er is geen mechanisme beschikbaar om de nieuwste informatiepositie over dreigingen te vertalen in aanvullende beveiligingsmaatregelen.
   Wij adviseren een versterking van de centrale organisatie bij RvIG met cybersecurity-medewerkers die een actuele informatiepositie bijhouden met betrekking tot cyberdreigingen gericht op de BRP. Daarbij valt te overwegen een Security Operating Center (SOC) in te schakelen, bijvoorbeeld bij DICTU, gericht op monitoring, technische kwetsbaarhedenanalyses (vulnerability scans), het uitvaardigen van richtlijnen voor actuele dreigingen etc.

3. **Onvoldoende awareness over cyberrisico's**
   De informatie uit de BRP is toegankelijk voor veel beheerders en gebruikers van de aangesloten systemen en de daaraan gekoppelde systemen.
   Wij constateren dat niet iedereen van hen op de hoogte is van de cyberrisico's en signalen over een mislukte of een geslaagde digitale inbraak daadwerkelijk oppakken.
   Het risico is dat beheerders en gebruikers fouten maken, die door kwaadwillenden worden benut.
   Wij adviseren de awareness over cyberrisico's van beheerders en gebruikers te verhogen bij de leveranciers en afnemers, namelijk de gemeenten, aangesloten overheidsinstanties en derden. Via gerichte educatieve acties dienen de beheerders en gebruikers van de BRP-gegevens zich meer bewust te zijn van de dreigingen en de noodzaak om eventuele afwijkingen te signaleren.

4. **Beperkt gebruik van de Baseline Informatiebeveiliging Overheid (BIO)**
   De BIO wordt alleen opgelegd aan overheidsinstanties, maar niet aan derden buiten de overheid.
   Wij constateren dat voor derden buiten de overheid geen richtlijnen worden voorgeschreven voor een minimaal in te richten niveau voor informatiebeveiliging en privacybescherming. Wij zien dit als een manco in de zorgplicht van de overheid, die bij alle afnemers zou moeten benadrukken dat zij zorgvuldig dienen om te gaan met privacygevoelige persoonsgegevens van de betrokkenen.
   Het risico is dat afnemende organisaties buiten de overheid onvoldoende beveiligingsmaatregelen treffen, waardoor kwaadwillenden kansen hebben om digitaal in te breken en zo een inbreuk kunnen maken op de privacy van betrokkenen.
   Wij adviseren het volgen van de BIO of de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems - Requirements' voor te schrijven voor de aangesloten leveranciers en afnemers buiten de overheid. De BIO en de ISO/IEC 27001:2013 beschrijven de minimale drempel voor de te treffen beveiligingsmaatregelen die moeten gelden voor alle aangesloten systemen en de daaraan gekoppelde systemen.

5. **Incomplete protocollering**
   De AVG vereist transparantie voor de betrokkenen, namelijk inzicht in welke persoonsgegevens waarvoor zijn gebruikt of waarom deze zijn gemuteerd, plus controleerbaarheid. In Sectie 4.2.1 'Protocollering van verstrekkingen' van het LO GBA staat een advies hoe de verwerkingen moeten worden geprotocolleerd in de gemeentelijke GBA-systemen en afnemerssystemen. Hierbij wordt onderscheid gemaakt naar te herleiden en niet te herleiden verstrekkingen. Te herleiden verstrekkingen zijn verstrekkingen op grond van een besluit (autorisatiebesluit van de verantwoordelijk Minister of gemeentelijke verordening) waarbij achteraf door het vergelijken van het besluit en de gegevens in het bestand van de bevraagde, zonder meer valt af te leiden wanneer welke gegevens aan welke instantie zijn verstrekt. Voorbeelden zijn uitgevoerde selecties of spontane gegevensverstrekking op basis van geplaatste afnemersindicaties op persoonslijsten. Niet te herleiden verstrekkingen zijn alle overige verstrekkingen, deze worden deels geprotocolleerd. Volgens het LO GBA is het niet nodig om het gebruik van gegevens door de afdeling Burgerzaken ten behoeve van verificatie van stukken en aangiften te protocolleren, evenals het gebruik van gegevens door de afdeling Burgerzaken ten behoeve van het maken van documenten die de afdeling zelf afgeeft, zoals paspoorten, rijbewijzen en dergelijke. Ook hoeven verstrekkingen aan de burger zelf niet te

worden geprotocolleerd.
Wij constateren dat niet is opgelegd dat de te herleiden verstrekkingen worden geprotocolleerd. Hierdoor is het niet mogelijk achteraf vast te stellen dat de verstrekkingen en mutaties terecht als 'te herleiden' zijn gemarkeerd en alleen door bevoegde functionarissen zijn geïnitieerd.
Wij constateren dat niet is opgelegd dat alle niet te herleiden verstrekkingen worden geprotocolleerd.
Wij constateren dat forensisch onderzoek naar illegale pogingen tot toegang of mutatie kan falen door de incomplete protocollering van de niet te herleiden verstrekkingen. Tevens is het nu niet mogelijk in het kader van periodieke monitoring steekproeven uit te voeren om de compliance met wet- en regelgeving te verifiëren. Door de incomplete vastlegging is er geen volledig inzicht in deze vorm van verstrekkingen.
Het risico is dat een kwaadwillende die persoonsgegevens opvraagt of muteert, kennis heeft van de wijze van protocollering, en zorgt dat malafide activiteiten binnen de categorieën vallen die niet worden geprotocolleerd.
Wij adviseren alle te herleiden en niet te herleiden verstrekkingen te protocolleren in de gemeentelijke GBA-systemen en de afnemerssystemen, zodat het mogelijk is achteraf hun rechtmatigheid te verifiëren. Bovendien geeft dit de mogelijkheid tot actieve monitoring via steekproeven en data analytics.

6. **Onvoldoende grip op autorisaties voor toegang van beheerders en gebruikers**
RvIG stelt geen eisen aan het autorisatiebeheer bij de gemeente of de afnemer.
Wij constateren dat door het ontbreken van eisen aan het autorisatiebeheer en de afwezigheid van gerichte monitoring en audits, niet kan worden vertrouwd op de integriteit van het autorisatiebeheer bij de aangesloten organisaties.
Het risico is dat misbruik van een enkele account van een beheerder of gebruiker leidt tot een inbreuk op de vertrouwelijkheid en mogelijk op de integriteit van de persoonsgegevens in de BRP, door de gedistribueerde opbouw van de systemen en gegevensverzamelingen.
Wij adviseren het centraal opleggen van strikte eisen voor autorisatiebeheer en wachtwoordbeleid voor beheerders en gebruikers bij de aangesloten systemen, aangevuld met monitoring en gerichte audits.

7. **Minimale wachtwoordlengte is te kort**
Het aangesloten systeem bij de afnemer, de gemeente of RNI krijgt toegang tot de GBA-mailbox server en GBA-V middels een naam en wachtwoord-combinatie. De functioneel beheerder bij de afnemer, de gemeente of RNI kan het wachtwoord wijzigen. Volgens het LO GBA dient een nieuw wachtwoord een lengte te hebben van minimaal 6 en maximaal 8 tekens.
Wij constateren dat de minimale wachtwoordlengte 6 tekens niet in compliance is met de Baseline Informatiebeveiliging Rijksdienst (BIR/TNK) norm 11.5.3, lid 1. Deze norm vereist voldoende sterke wachtwoorden. Momenteel is een wachtwoordlengte van minimaal 8 tekens gebruikelijk.
Wij adviseren de minimale wachtwoordlengte voor de GBA-mailbox server en GBA-V te verlengen van de huidige 6 tekens naar 8 tekens, om zo het raden en kraken van wachtwoorden moeilijker te maken voor een kwaadwillende.

8. **Onveilig beveiligingsprotocol SSL**
   De beveiliging van het GBA-netwerk is onder andere gebaseerd op het verouderde Secure Sockets Layer (SSL) protocol. Alle versies van SSL worden beschouwd als onveilig, sinds in oktober 2014 de POODLE-kwetsbaarheid bekend werd.
   Sinds 1999 is het Transport Layer Security (TLS) protocol beschikbaar op de markt. De actuele versie is TLS 1.2.
   Wij constateren dat binnen het GBA-netwerk het onveilige beveiligingsprotocol SSL wordt gebruikt.
   Het risico is dat kwaadwillenden gebruik kunnen maken van bekende zwakheden van SSL om het berichtenverkeer van het GBA-netwerk te kraken en daarin zelf te participeren.
   Wij adviseren over te stappen naar het beter beveiligde TLS 1.2-protocol, dat sinds augustus 2008 beschikbaar is. Indien technisch mogelijk, verdient het zelfs de voorkeur direct over te stappen naar de nieuwste versie TLS 1.3.

9. **Incomplete logging en monitoring**
   Protocollering is niet hetzelfde als logging. Protocolering is bedoeld om te voldoen aan de eisen van transparantie richting de persoon waarover gegevens zijn geregistreerd. Logging is het vastleggen van alle relevante gebeurtenissen, zodat beheerders later kunnen natrekken wie welke handelingen heeft uitgevoerd en waar fouten zijn opgetreden.
   Wij constateren dat de documentatie over de BRP weinig informatie verstrekt over logging en monitoring. Uit datgene wat beschikbaar is, krijgen wij de indruk dat centraal de vitale handelingen worden gelogd, maar krijgen wij geen beeld over actieve monitoring.
   Er is een generieke kwetsbaarheid bij veel organisaties, namelijk dat de gebeurtenissen in de lokale infrastructuur niet altijd op een afdoende wijze worden gelogd, en dat monitoring slechts in beperkte mate plaatsvindt. Indien er geen duidelijke richtlijnen worden gegeven voor wat minimaal nodig is aan logging en monitoring rondom de lokale systemen voor de BRP, is er een reële kans dat de lokale IT-beheerders hier onvoldoende aandacht aan besteden.
   Het risico is dat het bij of na een incident niet mogelijk is een forensisch onderzoek uit te voeren, aangezien er geen complete vastlegging bestaat.
   Wij adviseren het inrichten van een afdoende mate van logging van de gebeurtenissen binnen de lokale infrastructuur voor te schrijven voor de aangesloten gemeenten, overheidsinstanties en de afnemers buiten de overheid.
   Wij adviseren een steekproef uit te laten voeren bij een aantal aselect gekozen afnemers op logging en monitoring in de infrastructuur, om het risico van onvoldoende logging en monitoring te kwantificeren.

10. **Geen geanonimiseerde decentrale testgegevens**
    De documentatie over de BRP bevat richtlijnen voor een aansluittest, waarbij geanonimiseerde persoonsgegevens worden gebruikt. Er zijn echter geen centrale richtlijnen over het verbod om decentraal echte persoonsgegevens te gebruiken voor testen van op de BRP aangesloten systemen.
    Er is een generieke kwetsbaarheid bij veel organisaties, namelijk het gebruik van echte persoonsgegevens in de test- en acceptatieomgevingen voor lokale systemen. De motivatie hiervoor is dat een kleine groep beheerders toegang heeft tot de productieomgeving, en deze beheerders ook de test- en acceptatiewerkzaamheden uitvoeren. Daarom wordt het testen met (een kopie van) de productiegegevens lokaal niet als een risico ervaren.

Wij constateren dat door het ontbreken van centrale richtlijnen over het decentrale gebruik van testgegevens een reële kans bestaat dat sommige aangesloten organisaties handelen in strijd met de BIR/TNK norm 12.4.2 en AVG Art. 5, door te testen met productiegegevens. Het risico is dat persoonsgegevens uitlekken via de test- en acceptatieomgeving, bijvoorbeeld naar ondersteunende medewerkers van leveranciers of inhuurkrachten.
Wij adviseren de afnemers te wijzen op de noodzaak om productiegegevens te anonimiseren alvorens die als testgegevens te gebruiken in een acceptatieomgeving. Als compenserende maatregel is het mogelijk dat de gemeente of afnemersorganisatie specifiek beleid opstelt voor testen met productiegegevens, als zij daarbij een proces en toezicht inregelen om te voldoen aan de AVG. Een en ander is ter beoordeling van de lokale Functionaris voor de Gegevensbescherming (FG).
Wij adviseren een steekproef uit te laten voeren bij een aantal aselect gekozen afnemers op testen met persoonsgegevens uit de BRP, om het risico van uitlekken van persoonsgegevens via de test- en acceptatieomgevingen voor lokale systemen te kwantificeren.

11. **Onvoldoende robuustheid tegen aanval met ransomware of wiperware**
    Aanvallen op de overheid via sabotage zijn niet denkbeeldig. Sinds 2013 zijn minstens 170 Amerikaanse steden en overheidsdiensten getroffen door ransomware. De zorgen betreffen niet alleen besmetting met ransomware, waarna gegevens kunnen worden ontsleuteld na het betalen van losgeld, maar tevens besmetting met sabotagesoftware. De NCTV beschrijft het voorbeeld van de NotPetya sabotagesoftware. Dit bleek wiperware (software die gegevens wist), waarbij het onmogelijk was om de gegijzelde bestanden daadwerkelijk terug te krijgen.
    De meest gevaarlijke variant van wiperware nestelt zich in de systemen, zoekt uit hoe back-ups worden gemaakt en versleutelt op een bepaald moment zowel de gegevensverzamelingen als de recente back-ups. Hierdoor is een klassieke vorm van herstel niet direct meer mogelijk.
    Wij constateren dat Nederland niet is voorbereid op een dergelijke aanval op de BRP, onder andere door de gedistribueerde opzet en verantwoordelijkheden binnen de BRP.
    Het risico is dat na een succesvolle aanval met ransomware en wiperware de processen rondom burgerzaken bij de getroffen afnemers volledig worden verstoord. Indien systemen opnieuw moeten worden geïnstalleerd, verouderde niet getroffen back-ups moeten worden geladen, alle vanaf dat back-up-moment aangebrachte mutaties opnieuw handmatig moeten worden aangebracht en hersynchronisatie via GBA-V nodig is, kan de verstoringstijd oplopen tot maanden.
    Wij adviseren centraal richtlijnen op te stellen en uit te dragen voor het mitigeren van het risico van een besmetting van centrale en decentrale systemen met ransomware of wiperware, en zorg te dragen dat mitigerende maatregelen worden gerealiseerd bij de aangesloten partijen.

Wij adviseren het ministerie BZK verbeteracties te initiëren, die wij hebben samengevat en geprioriteerd in het Hoofdstuk ‘Overzicht van de adviezen’ hieronder.

## 3. Overzicht van de adviezen

De adviezen zijn hieronder samengevat. Wij maken in de kolom 'Prioriteit' onderscheid tussen korte termijn (op te lossen binnen 6 maanden), middellange termijn (op te lossen binnen 12 maanden) en lange termijn.

| Nr. | Advies | Prioriteit |
|---|---|---|
| 1 | **Geen actuele risicobeheersing**<br>Wij adviseren een versterking van de centrale organisatie bij RvIG met cybersecurity-medewerkers die een actuele informatiepositie onderhouden met betrekking tot cyberdreigingen gericht op de BRP. Daarbij valt te overwegen een Security Operating Center (SOC) in te schakelen, bijvoorbeeld bij DICTU, gericht op monitoring, technische kwetsbaarhedenanalyses (vulnerability scans), het uitvaardigen van richtlijnen voor actuele dreigingen etc. | Korte termijn |
| 2 | **Onvoldoende awareness over cyberrisico's**<br>Wij adviseren de awareness over cyberrisico's van beheerders en gebruikers te verhogen bij de leveranciers en afnemers, namelijk de gemeenten, aangesloten overheidsinstanties en derden. Via gerichte educatieve acties dienen de beheerders en gebruikers van de BRP-gegevens zich meer bewust te zijn van de dreigingen en de noodzaak om eventuele afwijkingen te signaleren. | Korte termijn |
| 3 | **Beperkt gebruik van de Baseline Informatiebeveiliging Overheid (BIO)**<br>Wij adviseren het volgen van de Baseline Informatiebeveiliging Overheid (BIO) of de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems - Requirements' voor te schrijven voor de aangesloten leveranciers en afnemers buiten de overheid. De BIO en de ISO/IEC 27001:2013 beschrijven de minimale drempel voor de te treffen beveiligingsmaatregelen die moet gelden voor alle aangesloten systemen en de daaraan gekoppelde systemen. | Korte termijn |
| 4 | Wij adviseren een steekproef uit te laten voeren bij een aantal aselect gekozen afnemers op logging en monitoring in de infrastructuur, om het risico van onvoldoende logging en monitoring te kwantificeren. | Korte termijn |
| 5 | **Geen geanonimiseerde decentrale testgegevens**<br>Wij adviseren de afnemers te wijzen op de noodzaak om productiegegevens te anonimiseren alvorens die als testgegevens te gebruiken in een acceptatieomgeving. Als compenserende maatregel is het mogelijk dat de gemeente of afnemersorganisatie specifiek beleid opstelt voor testen met productiegegevens, als zij daarbij een proces en toezicht inregelen om te voldoen aan de AVG. Een en ander is ter beoordeling van de lokale Functionaris voor de Gegevensbescherming (FG). | Korte termijn |
| 6 | Wij adviseren een steekproef uit te laten voeren bij een aantal aselect gekozen afnemers op testen met persoonsgegevens uit de BRP, om het risico van uitlekken van persoonsgegevens via de test- en acceptatieomgevingen voor lokale systemen te kwantificeren. | Korte termijn |

| Nr. | Advies | Prioriteit |
|---|---|---|
| 7 | **Incomplete protocollering**<br>Wij adviseren alle te herleiden en niet te herleiden verstrekkingen te protocolleren in de gemeentelijke GBA-systemen en de afnemerssystemen, zodat het mogelijk is achteraf hun rechtmatigheid te verifiëren. Bovendien geeft dit de mogelijkheid tot actieve monitoring via steekproeven en data analytics. | Middellange termijn |
| 8 | **Onvoldoende grip op autorisaties voor toegang van beheerders en gebruikers**<br>Wij adviseren het centraal opleggen van strikte eisen voor autorisatiebeheer en wachtwoordbeleid voor beheerders en gebruikers bij de aangesloten systemen, aangevuld met monitoring en gerichte audits. | Middellange termijn |
| 9 | **Minimale wachtwoordlengte is te kort**<br>Wij adviseren de minimale wachtwoordlengte voor de GBA-mailbox server en GBA-V te verlengen van de huidige 6 tekens naar 8 tekens, om zo het raden en kraken van wachtwoorden moeilijker te maken voor een kwaadwillende. | Middellange termijn |
| 10 | **Onveilig beveiligingsprotocol SSL**<br>Wij adviseren voor de beveiliging van het GBA-netwerk van het onveilige Secure Sockets Layer (SSL) protocol over te stappen naar het beter beveiligde Transport Layer Security (TLS) 1.2-protocol, dat sinds augustus 2008 beschikbaar is op de markt. Indien technisch mogelijk, verdient het zelfs de voorkeur direct over te stappen naar de nieuwste versie TLS 1.3. | Middellange termijn |
| 11 | **Incomplete logging en monitoring**<br>Wij adviseren het inrichten van een afdoende mate van logging van de gebeurtenissen binnen de lokale infrastructuur voor te schrijven voor de aangesloten gemeenten, overheidsinstanties en de afnemers buiten de overheid. | Middellange termijn |
| 12 | **Ontbreken van centrale aansturing en toezicht**<br>Wij adviseren bij de toekomstige ontwikkelingen van het BRP te overwegen af te stappen van de gedistribueerde structuur en over te gaan naar een centrale opslag van de persoonsgegevens die authentiek dienen te zijn. | Lange termijn |
| 13 | **Onvoldoende robuustheid tegen aanval met ransomware of wiperware**<br>Wij adviseren centraal richtlijnen op te stellen en uit te dragen voor het mitigeren van het risico van een besmetting van centrale en decentrale systemen met ransomware of wiperware, en zorg te dragen dat mitigerende maatregelen worden gerealiseerd bij de aangesloten partijen. | Lange termijn |

### *3.1. Kosten van de geadviseerde maatregelen*

Onderdeel van de opdracht is het presenteren van passende maatregelen ter mitigatie van de gesignaleerde risico's, inclusief een kosten-batenanalyse. In deze Sectie gaan wij in op de kosten.

Onze adviezen hebben betrekking op drie verschillende groepen maatregelen, namelijk:
- Strategisch / tactisch aanpak vanuit een meer centrale rolinvulling;
- Centraal te treffen technisch maatregelen;
- Decentraal te treffen maatregelen na een centrale opdracht.

#### *3.1.1. Strategisch / tactisch aanpak vanuit een meer centrale rolinvulling*

De maatregelen op strategisch / tactisch niveau betreffen de volgende adviezen:
- **Ontbreken van centrale aansturing en toezicht**
  Besluitvorming over het inrichten van een centrale organisatie die richtlijnen uitvaardigt voor actuele dreigingen op basis van een actuele informatiepositie, toezicht houdt en centrale logging en monitoring inricht, aangevuld met data analytics;
- **Onvoldoende grip op autorisaties voor toegang van beheerders en gebruikers**
  Het centraal opleggen van strikte eisen voor autorisatiebeheer en wachtwoordbeleid voor beheerders en gebruikers bij de centrale en aangesloten systemen, aangevuld met monitoring en gerichte audits;
- **Onvoldoende robuustheid tegen aanval met ransomware of wiperware**
  Het centraal opstellen van richtlijnen en deze uit te dragen voor het mitigeren van het risico van een besmetting van centrale en decentrale systemen met ransomware of wiperware, en zorg te dragen dat mitigerende maatregelen worden gerealiseerd bij de aangesloten partijen.

Het overnemen van deze adviezen is afhankelijk van de bereidheid van de opdrachtgever om risico's geheel of deels te accepteren, of die grotendeels te mitigeren. Mogelijke opties zijn:
- Een eerste scenario is te stellen dat de risico's voor de BRP nu bekend zijn, dat deze risico's de afgelopen jaren niet manifest zijn geworden en actie kan worden uitgesteld tot een daadwerkelijk incident optreedt;
- Een tweede scenario is het selecteren van een deelverzameling aan maatregelen, op basis van een risico versus kostenafweging;
- Een derde scenario is het starten van een project met als mogelijke naam 'Mitigatie cyberdreigingen BRP', om de uit deze adviezen volgende maatregelen te ontwikkelen en in continuïteit te implementeren.

Het tweede en derde scenario vereisen een uitbreiding van de centrale organisatie voor de BRP met security- en privacy-experts, om te zorgen voor een effectieve aansturing en gedegen toezicht. Tevens moet er aansluiting worden gezocht bij een Security Operating Center (SOC), bijvoorbeeld bij DICTU.

Voor de kosten van het derde scenario moet worden gedacht aan 2 à 3 extra medewerkers bij de centrale organisatie voor BRP en 2 à 3 cybersecurity experts en/of technical IT-auditors bij het SOC.

### *3.1.2. Centraal te treffen technische maatregelen*

De centraal te treffen technische maatregelen betreffen de volgende adviezen:

- **Minimale wachtwoordlengte is te kort**
  Het verlengen van de minimale wachtwoordlengte voor de GBA-mailbox server en GBA-V van de huidige 6 tekens naar 8 tekens;
- **Onveilig beveiligingsprotocol SSL**
  Het overstappen van het onveilige Secure Sockets Layer (SSL) protocol voor de beveiliging van het GBA-netwerk naar het beter beveiligde Transport Layer Security (TLS) 1.2- of 1.3-protocol.

De aanpassing van de wachtwoordlengte is een technische wijziging in de wachtwoordmodule in de centrale systemen, die moet worden uitgevoerd door de leverancier van de programmatuur. Het invoeren vereist communicatie met alle aangesloten organisaties, aangezien de beheerders van de aangesloten systemen met een wachtwoordlengte van 6 of 7 tekens hun wachtwoorden moeten aanpassen.

Het overstappen van SSL naar TLS vereist een onderzoek naar de technische afhankelijkheden en de realiseerbaarheid. Als de overstap mogelijk is, moet deze worden uitgevoerd door de leveranciers van het GBA-netwerk en de Public Key Infrastructure (PKI).

Deze kosten zijn in het kader van het huidige onderzoek niet te kwantificeren. Hiervoor dienen offertes te worden opgevraagd bij de leveranciers.

### *3.1.3. Decentraal te treffen maatregelen na een centrale opdracht*

De decentraal te treffen maatregelen, die centraal moeten worden opgelegd en worden gecontroleerd, betreffen de volgende adviezen:

- **Onvoldoende awareness over cyberrisico's**
  Het verhogen van de awareness over cyberrisico's van beheerders en gebruikers bij de leveranciers en afnemers, namelijk de gemeenten, aangesloten overheidsinstanties en derden;
- **Beperkt gebruik van de Baseline Informatiebeveiliging Overheid (BIO)**
  Het voorschrijven van het volgen van de Baseline Informatiebeveiliging Overheid (BIO) of de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems - Requirements' voor de aangesloten leveranciers en afnemers buiten de overheid;
- **Incomplete protocollering**
  Het voorschrijven van protocollering voor alle te herleiden en niet te herleiden verstrekkingen, zodat het mogelijk is achteraf hun rechtmatigheid te verifiëren;
- **Geen geanonimiseerde decentrale testgegevens**
  Het wijzen van de afnemers op de noodzaak om productiegegevens te anonimiseren alvorens die als testgegevens te gebruiken in een acceptatieomgeving of daarvoor een compenserende maatregel in te richten;
- **Incomplete logging en monitoring**
  Het voorschrijven van een afdoende mate van logging van de gebeurtenissen binnen de lokale infrastructuur voor de aangesloten gemeenten, overheidsinstanties en de afnemers buiten de overheid.

In feite betreffen deze adviezen maatregelen die de aangesloten organisaties zelf al hadden moeten treffen in het kader van een zorgvuldig beheer en het voldoen aan wet- en regelgeving, zoals de AVG.

Door het gebrek aan centrale aansturing en toezicht voldoen echter niet alle aangesloten organisaties aan de minimale eisen voor informatiebeveiliging en privacybescherming. Een hogere mate van compliance kan alleen worden bereikt door versterking van de centrale verantwoordelijkheid.

De overheid heeft gepoogd dit in te richten via bijvoorbeeld Eenduidige Normatiek Single Information Audit (ENSIA) voor de gemeenten. Naar onze mening levert ENSIA op dit moment echter te weinig zekerheid op over de awareness, logging en monitoring, en is onvoldoende effectief voor een gedegen implementatie van de BIO en anonimisering van testgegevens. Daarnaast geldt ENSIA alleen voor gemeenten, maar niet voor andere aangesloten organisaties.

De kosten voor deze maatregelen worden gedragen door de aangesloten organisaties en vallen binnen hun budget voor informatiebeveiliging en privacybescherming.

# 4. Opdrachtverantwoording

Op 1 maart 2019 hebben wij van de Directie I&O van het ministerie BZK de opdracht gekregen om een doorlichting van de digitale veligheid BRP uit te voeren in het kader van de Kamerbrief 'Verhogen informatiebeveiliging' van 16 oktober 2018.

## *4.1. De onderzoeksvraag*

De werkzaamheden zijn gericht op het inventariseren van de risico's en de maatregelen ter waarborging van de vertrouwelijkheid en integriteit van de gegevens in de BRP. Het accent ligt hierbij op de IT General Controls met betrekking tot toegang, wijzigingen en uitvoering ten aanzien van de applicatie GBA-V. De onderzoeksgebieden zijn in opzet en bestaan beoordeeld.

Het onderzoek betreft de situatie op 30 april 2019.

De conclusies en adviezen zijn in een rapport van bevindingen gepresenteerd aan de opdrachtgever.

## *4.2. De onderzoeksaanpak*

Wij hebben deze opdracht voor overeengekomen werkzaamheden uitgevoerd en hierover gerapporteerd conform de richtlijnen van de Nederlandse Orde van Register IT Auditors (NOREA).

**Fase 1 – Verkennend onderzoek voor scopebepaling en ontwikkelingen**

Op 12 maart 2019 zijn wij gestart met de Voorbereidingsfase, welke bestaat uit het opstellen van het werkprogramma en het uitvoeren van verkennende interviews. In april 2019 is documentatie verzameld via publiekelijk toegankelijke bronnen. De scope van het onderzoek is vastgesteld in overleg met de opdrachtgever.

**Fase 2 – Onderzoeksfase**

Wij hebben de deskresearch en diepgaande interviews uitgevoerd met specialisten en betrokkenen in de periode van 22 maart tot en met 24 april 2019. De bevindingen zijn in concept getoetst in overleg met de opdrachtgever of met de betrokkenen.

Er zijn gespreksverslagen gemaakt van de interviews en getoetst bij de geïnterviewden. Het dossier is zo opgezet dat de bevindingen traceerbaar zijn voor de opdrachtgever.

**Fase 3 – Analysefase en rapportage**

Aan de hand van de beschouwde documentatie en de uitgevoerde interviews zijn de onderzoeksvragen beantwoord. De uitgevoerde stappen zijn:

- Inventarisatie van de persoonsgegevens in opslag en transport;
- Globale inventarisatie van de reeds binnen de scope getroffen maatregelen voor de borging van de informatiebeveiliging en privacybescherming, en de mitigatie van (cyber)dreigingen;

- Dreigingsanalyse in de vorm van het identificeren van de mogelijke dreigende actoren (onder andere aan de hand van de jaarbeelden van NCSC en IBD), hun mogelijke modus operandi en de schade die zij zouden kunnen veroorzaken voor de rechten en belangen van de in BRP vermelde personen;
- Kwetsbaarheidsanalyse, waarbij de dreigingsscenario's zijn getoetst tegen het reeds ingerichte stelsel van maatregelen. Dit leidde tot de omschrijving van een mogelijk GAP tussen de IST (de getroffen maatregelen) en de SOLL (het door het kabinet gewenste niveau van beveiliging);
- Voorstellen van aanvullende mitigerende maatregelen op basis van de geconstateerde GAP, aangevuld met een inschatting van de effectiviteit, kosten en baten per maatregel.

De resultaten zijn vastgelegd in onze rapportage, waarvan het concept op 21 juli 2019 is overhandigd aan de Opdrachtgever. Dit concept is op 15 augustus, 30 augustus en 11 oktober 2019 besproken met de opdrachtgever.

### *4.3. Het onderzoeksteam*

De uitvoering van de werkzaamheden is verzorgd door:
- Prof.dr.ir. R. Paans RE (Ronald), hoogleraar verbonden aan de Postgraduate Opleiding IT Audit, Compliance & Advisory van de Vrije Universiteit en directeur Noordbeek;
- S.D. Kubacki (Sebastian), senior IT-auditor en teamleider;
- J. Winkel QSA CISA (Jerry), cybersecurityspecialist.

De eindverantwoordelijkheid voor de uitvoering van de opdracht berust bij ondergetekende.

### *4.4. Ondertekening*

Wij eindigen met een woord van dank voor de geïnterviewden, die naar onze mening op een open en transparante wijze alle door ons gevraagde informatie hebben verstrekt.

Hazerswoude, 18 oktober 2019

Prof.dr.ir. R. Paans RE

## Bijlage A Lijst van afkortingen

| Afkorting | Toelichting |
|---|---|
| AVG | Algemene Verordening Gegevensbescherming |
| BIG / BIO | Baseline Informatiebeveiliging Gemeenten / Overheid |
| BRP | Basis Registratie Personen |
| BSN | Burgerservicenummer |
| BV-BSN | Beheervoorziening BSN |
| BZK | Ministerie van Binnenlandse Zaken en Koninkrijkszaken |
| DIO | Directie Informatiesamenleving en Overheid (DIO), Ministerie BZK |
| ENSIA | Eenduidige Normatiek Single Information Audit |
| FG | Functionaris voor de Gegevensbescherming |
| GBA | Gemeentelijke basisadministratie persoonsgegevens |
| GBA-V | GBA Verstrekkingsvoorziening |
| IBD | Informatiebeveiligingsdienst |
| ICT | Informatie en Communicatie Technologie |
| IND | Immigratie- en Naturalisatiedienst, met haar informatiesysteem Indigo |
| LO GBA | Logisch Ontwerp GBA |
| NCSC | Nationaal Cyber Security Centrum |
| NCTV | Nationale Coördinator Terrorismebestrijding en Veiligheid |
| PGK | PIVA-GBA-Koppeling |
| PIVA | Persoonsinformatievoorziening Nederlandse Antillen en Aruba |
| RNI | Registratie Niet-Ingezetenen |
| RvIG | Rijksdienst voor Identiteitsgegevens |
| SOC | Security Operating Center |
| sPd-protocol | simple Protocol data. Dit protocol is ontwikkeld voor GBA, en is gebaseerd op het P7-protocol voor X.400. |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| TMV | Terugmeldvoorziening |