Oplegvel Collegebesluit

Portefeuille mr. B. B. Schneiders
Auteur Dhr. AGHP Jonkers
Telefoon 0235113187 E-mail: aghpjonkers@haarlem.nl
DV/PBO/2013/1739
GEEN bijlagen kopiëren
B & W-vergadering van 22 januari 2013

Onderwerp
Vaststelling Informatiebeveiligingsplan GBA en Waardedocumenten

DOEL: Besluiten

Artikel 2 Wet GBA: Het college van burgemeester en wethouders van elke gemeente is de verantwoordelijke voor de verwerking van persoonsgegevens over de bevolking in een geautomatiseerde basisadministratie van persoonsgegevens.
Artikel 14, lid 1Wet GBA: Het college van burgemeester en wethouders legt de hoofdlijnen van het beheer van de basisadministratie vast in een regeling die voor een ieder ter inzage wordt gelegd.

De Wet GBA wijst het college aan om de Beheerregeling BRP vast te stellen. De vaststelling van het Privacyreglement BRP is in de Verordening GBA door de raad gedelegeerd aan het college.

B&W

1. Stelt het Informatiebeveiligingsplan GBA en Waardedocumenten vast, inclusief Beheerregeling BRP en Privacyreglement BRP.
2. Trekt de Beheerregeling GBA in.
3. Trekt het Privacyreglement GBA in.
4. Het besluit heeft geen financiële consequenties.
5. De betrokkenen ontvangen na besluitvorming informatie over dit besluit; het Informatiebeveiligingsplan BRP wordt ter inzage gelegd.
6. De commissie Bestuur ontvangt het besluit van het college ter informatie.

Collegebesluit

Onderwerp: Vaststelling Informatiebeveiligingsplan GBA en Waardedocumenten
Reg. Nummer: DVL/PBO/2013/1739

1. Inleiding

Het is belangrijk dat de gemeente Haarlem beschikt over een goed en actueel Informatiebeveiligingsplan GBA en Waardedocumenten. Het huidige informatiebeveiligingsplan is geactualiseerd. Wijzigingen zijn aangebracht als gevolg van de veranderde huisvesting van de hoofdafdeling Dienstverlening en het daarmee samenhangende adres, de verplaatsing van servers van Haarlem naar een Service Center van KPN in Aalsmeer en de modernere wijze van het maken van back-ups. Geringe, maar noodzakelijke aanpassingen.
In het informatiebeveiligingsplan GBA en Waardedocumenten wordt het beleid vastgelegd van de informatiebeveiliging GBA. Daarnaast worden taken, verantwoordelijkheden en bevoegdheden van de beheerfuncties belegd, die inhoudelijk niet verschillen van hetgeen in het huidige informatiebeveiligingsplan is beschreven.

De beheerregeling is een belangrijk onderdeel van het informatiebeveiligingsplan. Sinds 1 januari 2010 geldt voor de hele overheid, en dus ook binnen gemeenten, de verplichting om bij de uitvoering van taken gebruik te maken van persoonsgegevens uit de GBA. Gemeentelijke afnemers dienen gegevens over de eigen inwoners te betrekken uit de ‘eigen basisadministratie’. Gegevens van ‘niet-inwoners’, die elders in de GBA zijn ingeschreven, moeten afkomstig zijn uit de basisadministraties van die andere gemeenten of uit de landelijke voorziening, de GBA-V. Deze nieuwe raadpleegfunctie van de landelijke GBA-V wordt uitgevoerd conform een autorisatiebesluit van het Ministerie van Binnenlandse Zaken, maar was tot dusverre nog niet geformaliseerd in de Beheerregeling.
Dit is de aanloop om, na vaststelling van de Wet basisregistratie personen, uiteindelijk te komen tot de basisregistratie personen (BRP) die de huidige GBA gaat vervangen. Om die reden is ervoor gekozen de nieuwe beheerregeling de ‘Beheerregeling BRP’ te noemen.

Het Privacyreglement met bijlages wordt ter vaststelling aangeboden. Bij de controle van het document is gebleken dat er een afnemer ontbreekt in de bijlage. Het Regionale Informatie en Expertise Centrum Noord-Holland (RIEC-NH) is nooit opgenomen in bijlage 1 van het privacyreglement. Op basis van een regionaal convenant is het RIEC-NH bevoegd tot inzage in GBA-gegevens en dit convenant is ook gemeld bij het College bescherming persoonsgegevens.
Gegevensverstrekking uit de GBA is daarmee legitiem maar nu is deze gegevensverstrekking ook opgenomen in bijlage 1 van het Privacyreglement BRP.

2. Besluitpunten college

1. Stelt het Informatiebeveiligingsplan GBA en Waardedocumenten vast, inclusief Beheerregeling BRP en Privacyreglement BRP.
2. Trekt de Beheerregeling GBA in.
3. Trekt het Privacyreglement GBA in.
4. Het besluit heeft geen financiële consequenties.
5. De betrokkenen ontvangen na besluitvorming informatie over dit besluit; het Informatiebeveiligingsplan BRP wordt ter inzage gelegd.
6. De commissie Bestuur ontvangt het besluit van het college ter informatie.

3. Beoogd resultaat

Met dit voorstel wordt bereikt dat de gemeente Haarlem beschikt over een actueel Informatiebeveiligingsplan GBA en Waardedocumenten.

4. Argumenten

4.1. Beleidsinhoudelijk

De gemeente Haarlem beschikt hiermee over een actueel informatiebeveiligingsplan GBA en Waardedocumenten, een actuele beheerregeling en een actueel privacyreglement.

4.2.Financieel

Dit besluit heeft geen financiële consequenties.

4.3. Communicatie

De terinzagelegging van het informatiebeveiligingsplan GBA en Waardedocumenten wordt bekendgemaakt.

5. Kanttekeningen

5.1. Juridisch

Geen opmerkingen

5.2. Communicatie

De documenten van het informatiebeveiligingsplan GBA en Waardedocumenten waarvan openbaarmaking de bedrijfsvoering schaadt, worden van openbaarmaking uitgesloten.

6. Uitvoering

De Beheerregeling BRP wordt gemeld bij het College bescherming persoonsgegevens.

7. Bijlagen

- Het Informatiebeveiligingsplan GBA en Waardedocumenten;
- De Beheerregeling BRP;
- Het Privacyreglement BRP met bijlages.

Het college van burgemeester en wethouders,

de secretaris de burgemeester

Informatiebeveiligingsplan GBA en Waardedocumenten

Gemeente Haarlem

Versie : 2.0

Status : definitief

Auteur : de heer G.H. Kalloe

Datum : 07-01-2013

BMC

Inhoudsopgave

1 Algemeen

1.1 Inleiding

In de gemeentelijke organisatie van Haarlem is een toenemend gebruik van geautomatiseerde informatiesystemen te constateren. In het algemeen zijn de gebruikers van deze systemen zich onvoldoende bewust van de risico's die worden gelopen ten aanzien van een ongestoord gebruik. Meestal onverwachts kan zich een calamiteit voordoen die het geautomatiseerde proces danig kan verstoren.

Voorliggend Informatiebeveiligingsplan is bedoeld om de risico's, verbonden aan het toenemend gebruik van computersystemen, zichtbaar te maken en aan te geven hoe deze risico's kunnen worden ingeperkt of beheersbaar gemaakt.

In dit Informatiebeveiligingsplan zijn de uitgangspunten en beveiligingsprocedures opgenomen die invulling geven aan al deze eisen.

1.2 Goedkeuring

Goedkeuring van dit basisdocument en de daarbij horende procedures vindt plaats nadat de betrokken personen van zowel de opdrachtnemer als opdrachtgever overeenstemming hebben bereikt over wat in het Informatiebeveiligingsplan staat beschreven.

Voor accordering van het voorliggend Informatiebeveiligingsplan tekent hieronder de opdrachtgever:

Gemeente Haarlem

College van B&W

Postbus 511

2003 PB Haarlem

Burgemeester, de heer B. Schneiders

Plaats en datum: Haarlem, ...

Handtekening:

Gemeentesecretaris, de heer J. Scholten

Plaats en datum: Haarlem, ...

Handtekening:

1.3 Versiebeheer

Versie	Datum	Auteur	Status	Aard wijzigingen	Verstuurd aan
1.1	05-03-2012	de heer G.H. Kalloe	Concept	1e concept	Viadesk
1.2	18-05-2012	de heer G.H. Kalloe	Concept	tekstueel	Viadesk
1.3	23-06-2012	de heer G.H. Kalloe	Concept	tekstueel	Viadesk
1.4	16-07-2012	de heer G.H. Kalloe	Concept	tekstueel	Viadesk
1.5	08-11-2012	de heer G.H. Kalloe	Concept	tekstueel	Viadesk
1.6	12-11-2012	de heer G.H. Kalloe	Concept	tekstueel	Viadesk
1.7		de heer G.H. Kalloe	Concept	tekstueel	Viadesk
2.0	07-012013	de heer G.H. Kalloe	Definitief	Ter vaststeling aangeboden	B&W, Viadesk
2.0	22-01-2013	de heer G.H. Kalloe	Definitief	Vastgesteld	Viadesk

1.4 Stuurgroep Burgerzaken

Ten behoeve van de totstandkoming van en periodieke afstemming (minimaal tweemaal per jaar) over dit Informatiebeveiligingsplan is door de gemeente Haarlem een (permanente) Stuurgroep Burgerzaken ingesteld.

Deze Stuurgroep Burgerzaken bestaat uit de volgende medewerkers:

- de teammanager balie hoofdafdeling Dienstverlening;
- de projectleider E-Dienstverlening hoofdafdeling Dienstverlening;
- de teammanager digiteam/telefoonteam/flexpool hoofdafdeling Dienstverlening;
- de gegevensbeheerder GBA;
- de applicatiebeheerder GBA;
- de beveiligingsfunctionaris reisdocumenten/rijbewijzen;
- de privacybeheerder GBA.

1.5 Geïnterviewden

Ten behoeve van de totstandkoming van het voorliggend Informatiebeveiligingsplan zijn in 2012 de volgende personen geïnterviewd:

- de gegevensbeheerder GBA;
- het hoofd ICT;
- de beveiligingsbeheerder;
- de Technisch beheerder Infrastructuur & Service.

De geïnterviewden hebben een sleutelrol in het beheer van de kernapplicatie GBA, in het beheer van waardedocumenten of in de (fysieke) beveiliging van het gemeentehuis.

1.6 Verantwoording

Voorliggend Informatiebeveiligingsplan is gebaseerd op de normen zoals vastgesteld in de Code voor Informatiebeveiliging. De Code is gebaseerd op de beste praktijkmethoden voor informatiebeveiliging zoals internationaal gebruikt in vele toonaangevende bedrijven.

Daarnaast is het voorliggend Informatiebeveiligingsplan gebaseerd op in aparte hoofdstukken opgenomen regelgeving.

1.7 Jaarlijkse actualisering

Het Informatiebeveiligingsplan en de aangedragen en genomen beveiligingsmaatregelen worden jaarlijks geëvalueerd en eventueel bijgesteld door de Stuurgroep Burgerzaken en daarna rechtstreeks aangeboden ter advisering aan het managementteam. Vervolgens wordt het geactualiseerde Informatiebeveiligingsplan aangeboden ter vaststelling aan het college van B&W.

1.8 Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt. De basis hiervoor is de beleidsdoelstelling van het Informatiebeveiligingsbeleid. Binnen de gemeente moeten medewerkers verantwoordelijkheden krijgen voor de implementatie van dit beleid.

De medewerkers worden betrokken (o.a. tijdens werkoverleg) bij de ontwikkeling en implementatie van zowel het beleid als de uitvoering.
Daarnaast wordt door de beveiligingsbeheerder vastgesteld of de maatregelen worden nageleefd. Verder wordt minimaal eenmaal per jaar het beleid geëvalueerd en eventueel herzien.
Het voorliggend Informatiebeveiligingsplan bevat tevens een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel wordt regelmatig gecontroleerd op actualiteit. In het Informatiebeveiligingsplan zijn daarom afspraken vastgelegd over de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen en procedures. De belangrijkste afspraak in dit verband is dat het voorliggend Informatiebeveiligingsplan en de daarbij behorende procedures en bijlagen jaarlijks opnieuw worden bekeken op actualiteit en dat de wijzigingen daarvan worden vastgesteld door het college van B&W, waarbij tevens wordt gecontroleerd op naleving van de beleidsuitgangspunten.
Daarnaast wordt het gehele beleid minimaal eenmaal per raadsperiode herijkt.

2 Beveiliging

2.1 Waarom beveiligen?

De gemeentelijke organisatie van Haarlem is in toenemende mate afhankelijk van een ongestoorde werking van haar informatiesystemen. Informatiesystemen zijn langzamerhand het zenuwcentrum geworden van de gemeentelijke organisatie.

Dat wordt gekarakteriseerd door:

- Probleemloos samenwerken van medewerkers op verschillende locaties.
- Het steeds groter worden van gegevensverzamelingen.
- De snelheid waarmee gegevens kunnen worden verwerkt.
- De (on)leesbaarheid voor de mens van vastgelegde gegevens.
- De éénmalige vastlegging ten behoeve van meerdere toepassingen en gebruikers.
- Concentratie van specifieke (informatiserings)kennis bij enkelen.

De kwetsbaarheid van de gemeentelijke informatiesystemen is dan ook een groot risico, waarvan de gemeentelijke organisatie van Haarlem zeer nadelige gevolgen kan ondervinden. Het is dus zaak door middel van zowel preventieve als repressieve beveiligingsmaatregelen de risico's zoveel mogelijk te beperken.

Maar het zijn niet slechts interne redenen waarom de gemeente Haarlem haar informatievoorziening moet beveiligen. Ook de wetgever stelt een aantal eisen. Door de Wet Bescherming Persoonsgegevens (WBP) worden eisen gesteld, waaraan gemeenten moeten voldoen en die zich richten tegen "verlies of enige vorm van onrechtmatige verwerking van gegevens". Onder onrechtmatige vormen van verwerking van gegevens vallen onder andere de aantasting van de gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot *alle* onderdelen van het proces van gegevensverwerking.

De gemeente Haarlem moet in het kader van de WBP "passende" beveiligingsmaatregelen nemen. In het begrip "passend" ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens.

Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van gegevens.

2.2 Wat beveiligen?

De functie van een informatiesysteem kan worden omschreven als het vastleggen, opslaan en verwerken van gegevens en het verstrekken van informatie. Beveiliging heeft daarom niet alleen betrekking op de hardware, maar ook op het gebruik ervan.

De informatiebeveiliging richt zich vooral op de volgende beveiligingsobjecten:

- Hardware en supplies.
- Software.
- Gegevens (data) en de verwerking daarvan.
- Datacommunicatie.
- Systeem- en applicatiedocumentatie.
- Het gebouw (het gemeentehuis inclusief dislocaties).
- Werkplek.
- Het (eigen) personeel.

De middelen die ten aanzien van deze beveiliging worden ingezet richten zich op het voorkómen, het ontdekken en het herstellen van de schade. De schade kan van materiële of immateriële aard zijn. De schade kan per ongeluk zijn ontstaan of opzettelijk zijn toegebracht.

Logische informatiebeveiliging is geen op zichzelf staande inspanning, maar maakt deel uit van de complete beveiliging. Een aantal maatregelen ligt dan ook in het verlengde van de al geldende beveiligingsmaatregelen, in het bijzonder waar deze betrekking hebben op de fysieke beveiliging van het gebouw en de werkplek.

In het kader van de Gemeentelijke basisadministratie zijn ten aanzien van de veiligheid van gegevens hoge eisen gesteld. Om aan die eisen tegemoet te kunnen komen dient, met respect voor de eigen omgeving, het beheer adequaat te zijn ingericht. Het begint met het onderwerpen van de eigen processen aan een stevige analyse. De analyse is er op gericht dat diverse bedreigingen in beeld worden gebracht. Vervolgens moet de kans op optreden van die bedreigingen zo effectief mogelijk naar een zo laag mogelijk niveau worden gebracht.

Beveiliging van gegevens vraagt om zorgvuldige analyses van de risico's die direct of indirect met die gegevens samenhangen. Gegevens kunnen verloren gaan, verminkt en daardoor onbetrouwbaar worden en in verkeerde handen vallen.

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

Om te komen tot een zo verantwoord mogelijke toepassing van informatiesystemen in de gemeentelijke organisatie van Haarlem is het van essentieel belang dat door het vaststellen van richtlijnen en procedures aangegeven wordt hoe de beheerders en gebruikers dienen om te gaan met de informatiesystemen.

In dit hoofdstuk wordt dieper ingegaan op de hoedanigheid van de verschillende beveiligingsobjecten.

2.2.1 Hardware

Onder hardware wordt verstaan:

- Server(s);
- Systeemconsole;
- Werkstations (inclusief beeldschermen, muis en toetsenbord);
- Laptops, pda's, smartphones;
- Extern geheugen zoals vaste schijven en schijvenpakketten;
- Tape-unit;
- UPS;
- Patchkast met bekabeling;
- Randapparatuur zoals printers, plotter, cd-rom spelers, tapestreamers, diskette units en paspoort- en rijbewijzenconfiguratie;
- Communicatieapparatuur;
- Supplies als tapes, cd's en memorysticks.

De hardware lijkt zo op het oog een nogal kwetsbaar beveiligingsobject. In fysieke zin is dit ongetwijfeld juist. Wel moet worden bedacht dat de hardware, in tegenstelling tot de software, vrij snel vervangbaar is, waarna het verwerkingsproces kan worden hervat. Zo is er voor de RS6000 een (respons) onderhoudscontract afgesloten door de gemeente Haarlem. Zie hiervoor de Bijlage Onderhoudscontract.

Een andere mogelijkheid is om het verwerkingsproces bij calamiteiten tijdelijk voort te zetten op bij het uitwijkcentrum aanwezige identieke hardware. De gemeente Haarlem heeft hiervoor intern de faciliteiten en mogelijkheden voor.

2.2.2 Software

De gemeente Haarlem heeft in verreweg de meeste gevallen standaard software aangeschaft. Daarom draagt de leverancier van de standaardprogrammatuur zorg voor beveiliging van de originele

programmatuur. Bij calamiteiten kan de beschadigde of verloren software in principe altijd worden vervangen. Dit laat onverlet dat de programmatuur regelmatig moet worden beveiligd.

Er is geen sprake van een eigen systeemontwikkeling. Mocht dit plaatsvinden, dan is het belangrijk te beseffen dat verlies van software niet alleen desastreus is voor de uitvoering van de werkzaamheden, maar ook, vanwege herprogrammering, belangrijke financiële nadelen oplevert. Voorkomen moet worden dat de software om welke reden dan ook verloren gaat.

De gemeente Haarlem gebruikt in het kader van voorliggend Informatiebeveiligingsplan op RS6000 de applicatie Probev van de leverancier Procura. Daarnaast wordt gebruikgemaakt van een in ontwikkeling zijnde webbased variant, Proweb. Het ligt in de lijn der verwachting dat Proweb op den duur de applicatie Probev volledig zal vervangen.

2.2.3 Gegevens

Gegevens zijn over het algemeen voor iedere organisatie uniek. Indien gegevens om wat voor reden dan ook verloren gaan kan men, tenzij men maatregelen heeft genomen, nergens meer op terugvallen. Reconstrueren van gegevens (voor zover mogelijk) is een kostbare en tijdrovende aangelegenheid.

Het is daarom van het grootste belang dat de gegevens elke werkdag worden gekopieerd naar een back-up medium, zodat bij calamiteiten de operationele versie van de data onmiddellijk kan worden vervangen door de laatst gemaakte kopie. De gebruikte methode voor het maken van een back-up is de zogenaamde generatiebeveiliging.

2.2.4 Datacommunicatie verbindingen

Onder verbindingen worden verstaan de communicatielijnen, draadloos of fysiek, die verschillende computers onderling met elkaar verbinden. Vooral zodra het openbare telefoonnet als communicatie-medium wordt gebruikt loopt men het risico dat onbevoegden het informatiesysteem binnendringen. Voor hackers gaat op dit punt echt geen zee te hoog en het is belangrijk daar ernstig rekening mee te houden. De enige afdoende beveiliging in deze situatie is de zogenaamde cryptografie, waarmee de over de communicatielijn te transporteren gegevens onleesbaar worden gemaakt voor onbevoegden. Voor het transport van bijvoorbeeld geheime data is cryptografie een “must”. Bij het transport van andersoortige data kan worden gehandeld als bij een niet op een openbaar netwerk aangesloten informatiesysteem.

In computersystemen die niet zijn gekoppeld aan het openbare net is het gevaar van inbreuk door externe onbevoegden minder aanwezig. Toch dient ook in dit geval een stelsel van identificatiecodes en wachtwoorden te voorkomen dat interne onbevoegden het systeem kunnen binnendringen.

Internet is in principe toegankelijk via de op het locale netwerk aangesloten pc’s.

Beveiliging tegen hackers is gewaarborgd via een eigen firewall. Daarnaast wordt een extra beveiliging nagestreefd met behulp van de virusscanner Sophos van Sophos. Zie hiervoor ook de Procedure Antivirus voorzieningen.

2.2.5 Documentatie

Onder documentatie wordt verstaan:

Systeemdocumentatie

- Hierin staat het doel en de werking van het computersysteem beschreven. Het betreft het volgende:
    - Configuratiebeschrijving;
    - Bekabelingsplan;
    - Contracten met de leveranciers;
    - Systeemhandboeken;

- o Aanwijzingen voor het onderhoud;
- o De te nemen acties bij storingen.

Gebruikersdocumentatie

- Hierin staat de werking van de diverse applicaties beschreven. Deze documentatie wordt door de applicatieleverancier beschikbaar gesteld.
- Ook voor de zelf ontwikkelde applicaties geldt dat er documentatie aanwezig dient te zijn.

De verantwoordelijkheid voor het bijhouden van de systeemdocumentatie ligt bij het hoofd ICT. De verantwoordelijkheid voor het bijhouden van de gebruikersdocumentatie ligt bij de applicatiebeheerder GBA.

2.2.6 Het gebouw

Het gemeentehuis van Haarlem is op een aantal manieren beveiligd. Er zijn voorzieningen getroffen ten behoeve van de fysieke beveiliging door de firma Alpha Security uit Haarlem. Hierbij is sprake van compartimentering van het gebouw. Tevens is er een inbraakdetecterende voorziening (stil alarm naar de meldcentrale van Alpha Security).

De kritische ruimten zijn afgesloten voor het publiek. In een gedeelte van het gemeentehuis zijn voorzieningen getroffen in de vorm van bewegingsmelders. Er is een elektronische toegangsbeveiliging voor het gemeentehuis. Tijdens avondopenstellingen is er slechts in beperkte mate maar voldoende controle op de toegang van het gebouw.

Beveiliging wil in dit verband ook zeggen: ontruiming in geval van brand- en/of bommeldingen.

Fysieke beveiliging dislocaties
Er is in de gemeente Haarlem geen dislocatie.

Kritische ruimten
Een kritische ruimte is een ruimte waarin een kwaadwillige zoveel schade kan aanrichten dat de beschikbaarheid van de informatiesystemen, die de gemeentelijke werkprocessen ondersteunen, kan worden verstoord. Een voorbeeld van een kritische ruimte is de computerruimte.
De volgende ruimten worden als kritisch beschouwd:

- Ruimte systeem- en netwerkbeheer;
- Computerruimte inclusief het Raasstation en patchkast;
- Kluisruimte back-up;
- Kluisruimte waardedocumenten;
- Werkruimten;
- Spreekkamers.

Daarnaast is de volgende ruimte aangewezen die weliswaar niet bedrijfskritisch is maar wel extra beveiligd moeten worden. Dit omdat de werkzaamheden welke er in worden uitgevoerd een groter diefstal en/of overvalrisico met zich meebrengen:

- Centrale kas.

2.2.7 Werkplek

De servers staan in de Raakspoort in een afzonderlijke, afgesloten computerruimte die zoveel mogelijk stofvrij is en waar een vorm van luchtbehandeling wordt toegepast. Daarnaast staan servers te Aalsmeer in een shared service center.

Uiteraard moet de computerruimte fysiek goed worden beveiligd. De werkplekken zelf (waar de werkstations staan) zijn fysiek minder goed te beveiligen. Hier moet worden teruggevallen op de algemene beveiligingsmaatregelen van de gemeente Haarlem.

De werkstations staan in de werkruimten en behoeven geen aparte luchtbehandeling.

2.3 Waar tegen moet worden beveiligd?

2.3.1 Inleiding

Computers kunnen worden geclassificeerd als technisch geavanceerde apparatuur en zijn daarmee ook gevoelig. Voor de gebruikers is het van groot belang dat kan worden vertrouwd op een ongestoorde werking. Ook gemeenten worden zo afhankelijk van hun informatiesystemen dat zij in het uitvoeren van hun taken bedreigd worden wanneer deze enige tijd niet zouden kunnen worden gebruikt (bijvoorbeeld door technische storingen of door brand).

Het staat vast dat de informatievoorziening ernstig zou zijn ontregeld als één of meer operationele informatiesystemen enige tijd niet zouden kunnen worden gebruikt (bijvoorbeeld het uitvallen van het informatiesysteem van Sociale Zaken met zijn berekenings- en betalingsruns of uitvallen van het GBA systeem met de daaraan gekoppelde dienstverlening naar de burger en landelijke afnemers).

Daar komt nog bij dat het belang en de kwetsbaarheid van computers en de waarde die ze vertegenwoordigen zo groot is dat dit soort installaties een uitermate geschikt doelwit zijn voor fraude, diefstal en sabotage. De ervaringen van enkele gemeenten in het verleden tonen aan dat dit niet louter theorie is.

Diverse voorzorgsmaatregelen kunnen ervoor zorgen dat het gevaar van grote stagnatie en extra kosten als gevolg van het uitvallen van een informatiesysteem tot een minimum wordt beperkt of zelfs wordt uitgesloten.

Een toenemende mate van afhankelijkheid van computers vraagt om een hogere mate van beveiliging van diezelfde computers.

2.3.2 Bliksem, brand en explosie

Bliksem is een groot gevaar voor gebouwen. Een blikseminslag kan een spanning bereiken van 100.000 Volt tot een stroomsterkte van 200.000 Ampère. Deze elektrische energie wordt binnen 50 tot 100 seconden vrijgemaakt en weer afgevoerd. Een blikseminslag van deze kracht veroorzaakt binnen een straal van 2 kilometer spanningspieken in de elektrische bedrading die elektronische apparaten kunnen beschadigen. Deze spanningspiek neemt af naarmate de afstand tot de inslag groter is.
Wanneer een gebouw direct wordt getroffen door de bliksem kan door de vrijkomende dynamische energie het fundament worden beschadigd. Ook kan er brand uitbreken.

Brand is een reëel en altijd aanwezig gevaar. Het is ook de meest voorkomende calamiteit. Brand kan fataal zijn voor gehele informatiesystemen. Naast directe schade kan vuur ook grote gevolgschade aanrichten. Het door de brandweer gebruikte bluswater beschadigt ook andere (veelal lager gelegen) delen van het door brand getroffen gebouw. De gebruikte apparatuur is hier erg gevoelig voor.
Bij de verbranding van, het in kantoorpanden veel gebruikte, PVC ontstaan chloorgassen die met het bluswater zoutzuurachtige verbindingen aangaan. Door het gebruik van klimaatbeheersingssystemen in kantoorpanden kunnen deze verbindingen door het gehele gebouw worden verspreid zodat ook de gevoelige elektronische apparatuur, die ver van de brandhaard staat opgesteld, wordt aangetast.

2.3.3 Stof, vuil en water

Computers zijn bijzonder gevoelig voor stof. Als gevolg van stof laten de filters in de koelelementen van computers steeds minder lucht door, waardoor de temperatuur op een gegeven moment te hoog kan oplopen. Voor servers geldt in het algemeen dat er maatregelen moeten worden genomen om de hoeveelheid aanwezige stof zoveel mogelijk te beperken. Een luchtbehandelinginstallatie is in dat geval onontbeerlijk. Voor pc's is dit in mindere mate het geval. Deze hardware is zo geconstrueerd dat er geen speciale voorzieningen nodig zijn. Regelmatig onderhoud is essentieel. Bij verwisseling van media (tapes, cd's en diskettes) kan gemakkelijk stofinfiltratie plaatsvinden. Al met al redenen om zoveel mogelijk te werken in een schone omgeving.

De oplossing hiervan wordt zichtbaar door rekening te houden met de volgende aanbevelingen. De apparatuur moet op een zodanige wijze worden geplaatst en beveiligd dat de risico's van schade, storing en aanraking met stof, vuil en water minimaal zijn.

Dit wordt bereikt door:

- Aandacht voor specifieke risico's, waaronder water, stof, trillingen, chemische reactie, interferentie met de elektriciteitsvoorziening en elektromagnetische straling;
- Verbod tot gebruik van etenswaren in kritische ruimten;
- Iedere medewerker er voor verantwoordelijk te houden zijn of haar eigen werkplek zoveel mogelijk stofvrij te houden;
- Het weren van zoveel mogelijk stofbronnen, zoals kartonnen dozen en bloembakken in de nabijheid van computerapparatuur.

Water in de gevoelige ICT apparatuur is verantwoordelijk voor kortsluiting, mechanische beschadiging en/of roestvorming. Doordat in de meeste kantoorgebouwen de telefooncentrale, de computerapparatuur, patchkasten en de hoofdverdelers voor de interne stroomvoorziening zijn gecentraliseerd in één fysieke ruimte, betekent waterschade in deze ruimte onmiddellijk een enorme schade.

Ongecontroleerde toestroom van water kan worden veroorzaakt door:

- Hoog water;
- Storing in het water(afvoer) systeem;
- Defect van het verwarmingssysteem;
- Defect van het klimaatbeheersingssysteem (airco);
- Defect van een sprinkler installatie;
- Bluswater van de brandweer.

2.3.4 Stroomuitval, storingen en fouten

Ondanks de verfijnde techniek en ondanks alle preventieve maatregelen kunnen er situaties ontstaan waarbij het informatiesysteem niet meer functioneert. Naast brand en explosie kunnen ook technische storingen de werking van het informatiesysteem ernstig verstoren.

Verfijnde apparatuur als netwerkservers zijn doorgaans gevoelig voor snelle temperatuurswisselingen. Vooral als het buiten heet is, kan veel apparatuur die is opgesteld in dezelfde computerruimte zijn warmte niet kwijt. De ruimte waar de computerhardware (servers/patchkast) staat is voorzien van airconditioning om een zo constant mogelijke temperatuur te waarborgen.

Ondanks de hoge kwaliteit van de Nederlandse stroomvoorziening, komt het toch op jaarbasis een aantal keren voor dat de stroom uitvalt. Meestal zal de stroomonderbreking niet langer duren dan een seconde zodat mensen het in het geheel niet opmerken. ICT apparatuur kan echter verstoord raken bij een stroomonderbreking langer dan 10 ms. Van stroomtoevoer zijn niet alleen de servers, pc's en verlichting afhankelijk, maar ook liften, buizenpost, telefoonapparatuur, beveiligingsapparatuur (brand en inbraak), airconditioning, verwarming en de watertoevoer in flats.
Storingen in de stroomvoorziening kunnen in principe worden ondervangen door het plaatsen van een zogenaamde UPS (Uninterruptible Power Supply) installatie. Hoewel dit een kostbare aangelegenheid is en de kwaliteit van de geleverde elektriciteit in Nederland goed te noemen is, is de hardware (zeker

de servers) zodanig storingsgevoelig dat een UPS een must is. Een UPS is te vergelijken met een flinke accu. Dankzij een UPS kan een server in geval van stroomuitval correct afgesloten worden.

Voor een doelmatige beveiliging is de duur van de 'down-time' van belang. Met down-time wordt bedoeld de tijd gedurende welke het informatiesysteem niet inzetbaar is. Is een langdurige systeemuitval van meer dan een paar dagen niet acceptabel, dan zal men moeten zorgen voor een “uitwijksysteem” op de werkplek zelf of in de directe nabijheid. In geval van de GBA moet de beschikbaarheid van de dienstverlening worden verzekerd naar de burger, de interne afnemers en de externe afnemers. Het is daarom wettelijk verplicht om voor de GBA een uitwijkcontract (zie bijlage Uitwijkcontract) en een eigen uitwijkprocedure (zie procedure Uitwijk) te hebben.

Door defecten, verkeerde bediening, ondeskundige wijziging of manipulatie en/of stroomuitval kunnen allerlei fysieke beveiligingsvoorzieningen uitvallen.

Het gevolg is:

- Defecte deursloten;
- Vervuilde brandmelders;
- Beschadigde sleutels of badges;
- Vastgeklemde regelcontacten in deuren;
- Ingebrande schermen van beveiligingsmonitoren;
- Uitval van modems en lijnverbindingen.

Dit soort problemen kunnen doorgaans niet worden opgelost door de gebruiker. Contact met de leverancier is in dat geval noodzakelijk.
Storingen aan de software kunnen een ernstig karakter krijgen als blijkt dat de software onverhoopt niet voorziet in bepaalde praktijksituaties. De enige vorm van beveiliging is hier een uitgebreide en diepgaande testperiode, voorafgaand aan de ingebruikneming van de software.
Een veel voorkomende groep van storingen wordt gevormd door printerstoringen. Deze zijn doorgaans snel oplosbaar, maar vormen een niet aflatende bron van irritaties voor de gebruikers.

2.3.5 Diefstal, sabotage, virussen en fraude door derden

Diefstal
Door de beperkte omvang van pc’s en zeker laptops is het voorkomen van diefstal van hardware een zaak geworden die wel degelijk aandacht verdiend. Immers, een laptop is al in een aktetas mee te nemen. En wat te denken van opslagmedia als tapecassettes, memorysticks en cd’s.

Er zijn echter nog andere risico’s verbonden aan onbevoegde aanwezigheid:

- Inzage door onbevoegden in privacygevoelige gegevens (documenten of dossiers);
- Manipulatie van papieren gegevens (zoals aanvraagformulieren);
- Manipulatie van geautomatiseerde gegevens;
- Diefstal van materiële eigendommen van medewerkers;
- Observaties (voorverkenning) waarmee criminele activiteiten kunnen worden voorbereid.

Fysieke beveiligingsmaatregelen in het kader van diefstal kunnen bestaan uit:

- Begeleiding van bezoekers;
- Fysieke legitimatieplicht (bijvoorbeeld zichtbaar dragen van badges);
- Afwezigheid van de aanduiding van kritische ruimten;
- Geen opslag van gevaarlijke stoffen in kritische ruimten;
- Aanwezigheid van detectiemiddelen en schadebeperkende voorzieningen in en rondom kritische ruimten;
- Compartimenteren van het gebouw met toegangsbeveiliging per compartiment.

Sabotage

Het saboteren van informatiesystemen kan zich op een fysieke en digitale manier voordoen. In het algemeen verstaan we onder sabotage het moedwillig verstoren van het geautomatiseerde verwerkingsproces.

Fysieke sabotage

Bij fysieke sabotage hebben we niet te maken met situaties die op een of andere manier te voorzien zijn, maar die voortkomen uit het falen van de techniek of een gevolg zijn van fouten en ongelukken.
Sabotage kan plaatsvinden door het eigen personeel of door onbekende personen die alleen of in groepsverband optreden met als doel de organisatie en haar werking te verstoren. Bescherming hiertegen is, temeer daar gemeentelijke gebouwen in principe een “open” karakter hebben, moeilijk.

Het is wel wenselijk geen hardware in de nabijheid van ramen te plaatsen. Bevinden computers zich op de begane grond, dan is het aan te bevelen, ter voorkoming van het ingooien van ruiten, de ramen te voorzien van slagvast glas.

Digitale sabotage

Een bijzondere vorm van sabotage zijn virussen. De grootste bedreiging voor pc’s is dat deze via internet onverhoeds een computervirus oplopen. Internet kent een groot aantal verschillende virussen. Zo zijn er de zogenaamde Trojaanse paarden: besmette programma's die verstopt zitten in andere programma's. De meeste virussen tasten de gegevens op de harde schijf aan, zodat belangrijke informatie verloren gaat, maar er zijn ook virussen die gehele pc’s in één keer ruïneren.
Over het algemeen verspreiden computervirussen zich als bijgevoegde bestanden bij e-mail en via programma's die van internet zijn te downloaden. Virussen zitten verstopt in besmette computerprogramma's die heel gewoon lijken, bijvoorbeeld een screensaver of een spelletje. Zodra u een programma opent dat besmet is met een virus, wordt dit virus actief en kan het veel schade berokkenen. Uw computer kan geïnfecteerd raken met een virus via valse bestanden of via onbetrouwbare webpagina's.

De beste verdediging tegen virussen en Trojaanse paarden is het gebruik van een anti-virusprogramma. Het is hierbij erg belangrijk dat er regelmatig een recente viruslijst wordt gedownload van de webpagina van de leverancier Sophos van de anti-virussoftware Sophos.

Verder is het van groot belang dat er geen onbekende bestanden worden geopend of gedownload. Dit geldt ook voor beveiligingssoftware die u kunt downloaden van internet. U zult helaas niet de eerste zijn die denkt een goede beveiliging aan te leggen, maar in werkelijkheid beveiligingssoftware installeert die zelf besmet blijkt te zijn met een virus of een Trojaans paard.

Fraude door derden

Door fraude kunnen criminelen reisdocumenten en/of rijbewijzen op een valse naam verwerven. Ook kan door fraude diefstal worden gemaskeerd.
In de praktijk worden verschillende fraudevormen onderscheiden:

Fraude zonder medewerking (misleiding)

Hierbij proberen kwaadwillenden een document te verkrijgen onder een valse naam door medewerkers te misleiden. Er wordt onderscheid gemaakt tussen *aanvraag op oneigenlijke gronden* en aanvragers die zich voordoen als een ander (*look-alike*).
Bij een aanvraag op oneigenlijke gronden maakt een (illegale) persoon bij de aanvraag van een nieuw document gebruik van de personalia van een persoon die is ingeschreven in de GBA. Indien deze aanvraag wordt toegekend, wordt een document afgegeven waarvan de foto niet overeenkomt met de personalia in het document. Bij een dergelijke fraudepoging zal de aanvrager (fraudeur) over het algemeen het oude document niet overleggen, maar gebruik maken van een ten onrechte opgemaakt proces-verbaal.
Look-alikes presenteren zich meestal bij grenscontroles, inschrijvingen bij uitzendbureaus en aanvragen van sociale uitkeringen. Maar ook op gemeentehuizen proberen look-alikes soms onder overlegging van een document van een ander een nieuw reisdocument te verwerven. De look-alike probeert een nieuw document te verwerven door zich voor te doen als degene van wie hij een correct afgegeven oud document bezit. De aanvrager lijkt sterk op de foto in dit oude document. Het document dat de fraudeur gebruikt, is dikwijls een vermist document dat in het criminele circuit is terechtgekomen of dat door de houder aan de fraudeur ter beschikking is gesteld.

Fraude onder druk
Hierbij proberen kwaadwillenden een document te verkrijgen op een valse naam door met chantage, bedreiging of omkoping de medewerking van medewerkers af te dwingen.

Interne fraude
Hierbij plegen medewerkers op eigen initiatief onrechtmatige handelingen of werken zij daar bewust aan mee.

2.3.6 Onbevoegd gebruik door derden

Onbevoegd gebruik van computersystemen kan zich in velerlei vormen voordoen, van computerspelletjes tot zelfs privé-administraties aan toe. Omdat in de gemeentelijke organisatie de hardware decentraal is opgesteld, is onbevoegd gebruik moeilijk te constateren.

Het onbevoegd gebruik van de hardware door onbekende individuen of personeel van andere afdelingen moet in eerste instantie door fysieke beveiliging worden voorkomen. In tweede instantie kan gebruik gemaakt worden van beveiligingssoftware. Door aan het informatiesysteem kenbaar te maken welke gebruikers toegang hebben tot het informatiesysteem en welke bevoegdheden deze gebruikers hebben, wordt een drempel gelegd voor potentiële fraudeurs.

Het principe van de meeste beveiligingssoftware berust op een autorisatiematrix. Daarin is vastgelegd welke objecten beveiligd moeten zijn tegen welke handelingen van welke gebruikers. De veiligste methode is “niets toestaan tenzij uitdrukkelijk anders is bepaald”. Alle handelingen van de gebruikers kunnen dan worden getoetst op rechtmatigheid.

Om toegang te krijgen tot een informatiesysteem moet de gebruiker zich identificeren met een gebruikersidentificatie en een wachtwoord. Deze combinatie - die binnen een systeem uniek is - wordt getoetst aan de autorisatiematrix. Komt deze combinatie niet in de matrix voor, dan krijgt de gebruiker geen toegang tot het systeem. Zijn poging om het informatiesysteem binnen te komen wordt geregistreerd in het logboek en geeft de Technisch beheerder Infrastructuur & Service de gelegenheid een passende actie te nemen, bijvoorbeeld een verscherpte controle op het gebruik van het betreffende werkstation of het veranderen van identificatie en wachtwoord.

Heeft de geautoriseerde gebruiker eenmaal toegang tot het systeem verkregen, dan zal hij gebruik willen maken van software en data. Het zal duidelijk zijn dat, naast de software, ook de in het systeem opgeslagen data beveiligd moet zijn tegen een onbevoegd gebruik (lezen, wijzigen of afdrukken). Ook dit kan in de autorisatiematrix worden opgenomen.

Opgemerkt wordt nog dat geen garantie kan worden gegeven voor een sluitende beveiliging. Een goede beveiliging is grotendeels afhankelijk van de discipline van de gebruikers en de controle daarop. Er moet zorgvuldig worden omgegaan met het gebruik van de autorisatiegegevens. Het laten slingeren van deze gegevens is te vergelijken met een huis dat wordt afgesloten en waarvan de sleutel naast het deurslot wordt gehangen.

2.3.7 Fraude door eigen personeel

De gegevensverwerking bij de gemeente Haarlem vindt vrijwel geheel plaats via computersystemen. Dit impliceert dat functies die rechtstreeks verband houden met geautomatiseerde gegevensverwerking, zoals die van de Technisch beheerder Infrastructuur & Service en de applicatiebeheerders, steeds meer het karakter krijgen van vertrouwensfuncties.

Daar komt nog bij dat systeem- en applicatiebeheer, gezien het specialistische karakter, moeilijk aan toezicht te onderwerpen is, zowel voor wat betreft de technische juistheid van de uitvoering als de rechtmatigheid van de verrichte handelingen.

Uit het oogpunt van beschikbaarheid mag het systeembeheer en het applicatiebeheer niet exclusief worden opgedragen aan één persoon. Onverhoopt vertrek van de Technisch beheerder Infrastructuur & Service - en daarmee het vertrek van alle kennis van het betreffende informatiesysteem - kan ernstige beschikbaarheidproblemen opleveren. Daarom is het aan te bevelen minimaal één plaatsvervanger aan te wijzen en die van tijd tot tijd de systeembeheerstaak te laten vervullen. Hetzelfde geldt uiteraard voor de applicatiebeheerders.

De ervaringen hebben aangetoond dat de grootste potentiële dreiging voor een informatiesysteem schuilt in het personeel dat daarvan gebruik maakt.

Daarom is een nauwkeurige selectie van personeel dat uitvoeringsverantwoordelijkheid gaat dragen voor computersystemen een aanbeveling. Daarbij moet vooral worden gelet op eigenschappen als verantwoordelijkheidsgevoel, discipline en integriteit. Hierbij kunnen een antecedentenonderzoek, diplomacontrole en natrekken van de opgegeven referenties een rol spelen.

Functiescheiding

Functiescheiding is het uit controle-overwegingen aanbrengen van een splitsing in taken en bevoegdheden die samenhangen met administratief handelen, over verschillende daartoe aangewezen functionarissen. Het doel is om ervoor te zorgen dat 2 opeenvolgende kritische stappen niet door dezelfde persoon worden uitgevoerd. De nadruk ligt op het voorkómen van fraude door externen of door interne medewerkers, al dan niet onder druk van kwaadwillenden (chantage, bedreiging of omkoping).

In de praktijk overtreft het aantal te scheiden taken vrijwel altijd het aantal medewerkers. Van een 1-op-1 functiescheiding zal daarom zelden sprake zijn. Optimale functiescheiding wordt verkregen door het zoveel mogelijk verdelen van de taken over de beschikbare medewerkers. Zie voor de concrete effectuering van de functiescheiding Bijlage Functieverdeling.

3 Informatiebeveiligingsbeleid

3.1 Beleidsdoelstelling

Beleid wordt gedefinieerd als een min of meer weloverwogen streven om bepaalde doeleinden met bepaalde middelen binnen een bepaalde tijdsvolgorde te bereiken.

Het college van B&W van de gemeente Haarlem stelt zich ten aanzien van de informatiebeveiliging als doelstelling die beveiligingsmaatregelen te treffen die enerzijds uit de wettelijke verplichtingen voortvloeien en anderzijds de beschikbaarheid, data integriteit, vertrouwelijkheid en controleerbaarheid van de gemeentelijke bedrijfsprocessen zoveel mogelijk garanderen. Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het college van B&W van de gemeente Haarlem de uiteindelijke verantwoordelijkheid draagt.

3.2 Wettelijke verplichtingen

Ten aanzien van de beveiliging van persoonsgegevens geldt artikel 13 van de Wet bescherming persoonsgegevens (Wbp) als grondslag voor het Informatiebeveiligingsbeleid. De tekst van dit artikel luidt:

> *De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*

Het College Bescherming Persoonsgegevens (CBP) kan de verantwoordelijke, in casu het college van B&W, aanspreken op het niveau van de maatregelen voor de beveiliging van de verwerking van persoonsgegevens en de wijze waarop het stelsel van maatregelen is geïmplementeerd en wordt nageleefd.

3.2.1 Fysieke beveiliging

Volgens de Inleiding EDP-auditing [1] moet het beveiligingsbeleid ten aanzien van de fysieke beveiliging in ieder geval de volgende onderdelen bevatten:

1. Doel van de beveiliging uitgaande van de bestaande organisatie voor de nabije toekomst.
2. Objecten welke beveiligd zouden moeten worden.
3. Richtlijnen voor de wijze waarop beveiliging van de relevante objecten kan worden gerealiseerd.

Ad 1) In de doelstelling moet worden aangegeven op welke termijn het beleid moet zijn uitgevoerd en tegen welke bedreigingen beveiliging noodzakelijk is. In dit deel van het Informatiebeveiligingsplan is in hoofdstuk 2 aangegeven tegen welke bedreigingen er beveiligd moet worden. In de bijlage risico inventarisatie en evaluatie GBA is per risicogroep concreet aangegeven welke beveiligingsmaatregelen zijn of zouden moeten worden getroffen.

Ad 2) Waar gegevens bij uitstek het beveiligingsobject zijn van het Informatiebeveiligingsbeleid, zijn het gebouw, het personeel en de werkplekken de beveiligingsobjecten van het fysieke beveiligingsbeleid.

Ad 3) De richtlijnen voor het fysiek beveiligen van de objecten zijn door de gemeente Haarlem gedetailleerd in de Bijlage Risico inventarisatie en evaluatie GBA beschreven.

[1] Zie Jan van Praat & Hans Suerink, Inleiding EDP-auditing, Kluwer Bedrijfsinformatie Deventer, januari 2001, ISBN 90 440 0199 X.

3.2.2 Informatiebeveiliging

Informatiebeveiligingsbeleid is volgens de Code voor Informatiebeveiliging[2] het op schrift gestelde en door het gemeentebestuur en het managementteam goedgekeurde beveiligingsbeleid met betrekking tot de informatievoorziening met hierin een formulering van de volgende elementen:

1. Een definitie van de term "informatiebeveiliging".
2. Een beschrijving van de belangrijkheid van informatiebeveiliging ten aanzien van het primaire proces.
3. Een verklaring over de betrokkenheid van het managementteam met betrekking tot informatiebeveiliging.
4. Een beschrijving van de algemene en specifieke verantwoordelijkheden voor alle aspecten van informatiebeveiliging binnen de organisatie.
5. Een bepaling over de frequentie waarmee dit document opnieuw beoordeeld moet worden.
6. Uitspraken over confirmatie aan de door de wetgever gestelde eisen.

Ad 1) Onder informatiebeveiliging wordt in dit kader verstaan een samenhangend geheel van maatregelen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens garandeert evenals de controleerbaarheid van de getroffen maatregelen. Als beleidsdoelstelling wordt de eis neergelegd dat de informatiesystemen aangeduid in voorliggend plan een beschikbaarheid tijdens werktijd kennen van minimaal 95%. Buiten werktijd worden er geen eisen gesteld aan de beschikbaarheid met uitzondering van voorzieningen in het kader van rampenbestrijding.

Ad 2) De gemeentelijke bedrijfsvoering van Haarlem komt onmiddellijk in problemen wanneer er inbreuk wordt gemaakt op de informatiebeveiliging. Dat betekent dat het primaire proces slechts uitgevoerd kan worden wanneer het niveau van informatiebeveiliging op een voldoende hoog niveau wordt belegd. Bedreigingen kunnen we nimmer wegnemen. De kans op het voorkomen van bedreigingen kan echter kleiner worden gemaakt door het treffen van preventieve maatregelen. De (gevolg)schade die wordt geleden kan worden beperkt door repressieve- en herstelmaatregelen.

Ad 3) Zie het vervolg van dit hoofdstuk voor een verklaring over de betrokkenheid van het gemeentebestuur en het managementteam met betrekking tot informatiebeveiliging.

Ad 4) Zie het vervolg van dit hoofdstuk voor uitspraken over de verantwoordelijkheden zoals het managementteam die ziet.

Ad 5) Dit document wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de beveiligingsbeheerder en bij noodzaak daartoe bijgesteld. Alle medewerkers van de gemeente worden via de gebruikelijke interne kanalen en voor zover noodzakelijk door hun leidinggevende via het reguliere werkoverleg geïnformeerd over voor hen van belang zijnde wijzigingen in beveiligingsbeleid, -plan, -maatregelen en/of –procedures.
Alle wijzigingen die direct betrekking hebben op individuele taken en bevoegdheden worden expliciet door de leidinggevende met zijn of haar betrokken medewerker(s) rechtstreeks gecommuniceerd.

Ad 6) De gemeente Haarlem zal zich houden aan de bepalingen van de in het kader van informatiebeveiliging relevante wet- en regelgeving zoals het Wetboek van Strafrecht, het Wetboek van Strafvordering (Wet computercriminaliteit), evenals de relevante regelgeving.

Beveiliging is geen doel op zich, maar een middel. De kosten moeten opwegen tegen de baten. De baten zijn echter moeilijk meetbaar. Het beveiligingsbeleid zal nauw moeten aansluiten op de cultuur van de gemeentelijke organisatie, de eigen bedrijfsprocessen en de binnen de organisatie

[2] Zie de Code voor Informatiebeveiliging 2000, Een leidraad voor beleid en implementatie, Nederlands Normalisatie Instituut te Delft 2000, ICS 35.020, SPE norm 20003.

gehanteerde terminologie. Dit alles zal de acceptatie en toepassing van het beveiligingsbeleid sterk verhogen.

3.2.3 Raakvlakken met ander beleid

Het Informatiebeveiligingsbeleid heeft raakvlakken met het beleid en de daaruit voortvloeiende procedures die zijn gericht op de operationele veiligheid van het uitgifte en beheerproces van waardedocumenten.

Informatiebeveiligingsbeleid maakt deel uit van het totale beveiligingsbeleid van de gemeente Haarlem. Binnen dit beleidsterrein kan er onderscheid worden gemaakt tussen fysieke toegangsbeveiliging, identificatie van gebruikers (logische toegangsbeveiliging, sleutelbeleid, personeelsbeleid, integriteitsbeleid en een clean desk/clear screen policy).

3.3 Taken, verantwoordelijkheden en bevoegdheden

De verantwoordelijkheid voor het Informatiebeveiligingsplan ligt altijd bij de verantwoordelijke, het college van B&W.
Deze stelt het Informatiebeveiligingsplan op en ziet toe op de uitvoering ervan door de betreffende medewerkers.
De beveiligingsbeheerder is verantwoordelijk voor het toezicht op de naleving van de beveiligingsmaatregelen en –procedures van het Informatiebeveiligingsplan en ziet erop toe dat eens per jaar gecontroleerd wordt of de nog te nemen maatregelen gerealiseerd zijn en dat het Informatiebeveiligingsplan hierop aangepast wordt.

Voor alle in dit Informatiebeveiligingsplan voorkomende functies is in Bijlage Functieverdeling de vervanging vastgelegd.

3.3.1 Verantwoordelijkheden gemeentebestuur

Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Haarlem. Het college van B&W stelt dit Informatiebeveiligingsplan vast.

Het college van B&W onderschrijft volledig de beveiligingsmaatregelen die in dit Informatie-beveiligingsplan worden voorgeschreven en wenst dat de stand van zaken met betrekking tot de informatiebeveiliging jaarlijks wordt geëvalueerd om er zorg voor te dragen dat de informatiebeveiliging in de gemeente up-to-date blijft.

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

Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van onderhavig Informatiebeveiligingsplan is de functie van beveiligingsbeheerder in het leven geroepen. Deze heeft de verantwoordelijkheid toe te zien op naleving van de beveiligingsmaatregelen en –procedures zoals uitgewerkt in voorliggend Informatiebeveiligingsplan en daarover aan het college van B&W te rapporteren.

De functie van de beveiligingsbeheerder moet niet verward worden met de functie van ‘de beveiligingsfunctionaris reisdocumenten’ noch met die van ‘de beveiligingsfunctionaris rijbewijzen’. Beide laatstgenoemde functies kennen zeer specifieke taken en verantwoordelijkheden op het beveiligingsgebied van enerzijds de reisdocumenten en anderzijds de rijbewijzen. De inhoud van beide functies zal apart worden toegelicht.

3.3.2 Verantwoordelijkheden van het managementteam

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle leden van het managementteam van de gemeente Haarlem.

Het managementteam bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

Per jaar zullen de volgende punten met betrekking tot beveiliging aan de orde komen:

- Voortgang realisatie beveiligingsmaatregelen als beschreven in het Informatiebeveiligingsplan en gerapporteerd door de beveiligingsbeheerder;
- Mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen;
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingsbeheerder;
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingsfunctionaris reisdocumenten en/of de beveiligingsfunctionaris rijbewijzen;
- Goedkeuring van initiatieven om de (informatie)beveiliging te verbeteren;
- Geven van voor een ieder zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen;
- Bevorderen van het beveiligingsbewustzijn;
- Herziening en goedkeuring beveiligingsbeleid en de toegekende verantwoordelijkheden.

3.3.3 Verantwoordelijkheden van de beveiligingsbeheerder

Door het college van B&W is de beveiligingsbeheerder benoemd. De beveiligingsbeheerder is verantwoordelijk voor het beheer van en het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Informatiebeveiligingsplan. De beveiligingsbeheerder rapporteert periodiek (minimaal eens per jaar) aan het college van B&W en het managementteam, zo nodig zonder tussenkomst van de diverse afdelingsmanagers.

Onder beveiligingsbeheerder wordt verstaan: een medewerker die kennis en ervaring heeft op het gebied van informatiebeveiliging en op dit terrein een adviserende en coördinerende rol kan vervullen.

De beveiligingsbeheerder is verantwoordelijk voor:

- Toezicht op de voorbereiding, implementatie en uitvoering van het beveiligingsbeleid en –plan;
- Een jaarlijkse rapportage over de voorbereiding, implementatie en uitvoering van het beveiligingsbeleid en –plan aan het college van B&W en het managementteam;
- Rapportage van beveiligingsincidenten;
- Het toezicht op de naleving van de beveiligingsprocedures;
- Toezicht houden op het feit dat minstens eenmaal per jaar voorlichting of instructie aan medewerkers wordt verzorgd, door middel van toetsing van de opgestelde beveiligingsprocedures in de praktijk;
- Toezicht houden op het feit dat nieuwe medewerkers worden geïntroduceerd en bekend worden gemaakt met de beveiligingsprocedures.

De beveiligingsbeheerder verstrekt daarnaast gevraagd en ongevraagd adviezen om te komen tot het gewenste beveiligingsniveau.

3.4 Passende technische en organisatorische maatregelen

Welk niveau van technische en organisatorische maatregelen passend is wordt bepaald door de risicoklasse, waarin de persoonsgegevens worden ingedeeld.
De in de GBA vastgelegde persoonsgegevens zijn op grond van de door het College bescherming persoonsgegevens (CBP) gehanteerde classificatie ingedeeld in risicoklasse II (verhoogd risico), dat wil zeggen er bestaan in vergelijking met het basisniveau van risicoklasse I extra negatieve gevolgen voor de betrokkenen bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De indeling in deze risicoklasse komt voort uit de aard van de gegevensverwerking in de GBA: de gegevens die worden verwerkt hebben betrekking op de gehele bevolking van de gemeente Haarlem.

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 risico's welke verbonden zijn met de gedefinieerde risicoklasse.

De te nemen maatregelen worden gewogen aan de hand van de volgende criteria:
- Stand van de techniek;
- Kosten;
- Risico's zowel van de verwerking, de aard als van de omvang van de persoonsgegevens.

3.4.1 Kwaliteitsaspecten

Informatiebeveiligingsbeleid is niets anders dan een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijke top eendrachtig duidelijk maken aan het tactische en operationele niveau welke gedragslijn de gemeente Haarlem dient te volgen om te komen tot een adequate informatiebeveiliging. Het beleid vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Het maken en vaststellen van beveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten in een Informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het management vast te stellen of de maatregelen werken. Evaluatie van het beleid dient vervolgens plaats te vinden om na te gaan of het beleid nog steeds aansluit op de organisatie en of de juiste maatregelen zijn getroffen.

De beveiliging van persoonsgegevens kent vier kwaliteitsaspecten, namelijk:

1e: beschikbaarheid	De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.
2e: integriteit	De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
3e: vertrouwelijkheid	Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.
4e: controleerbaarheid	Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trail) van groot belang. Controleerbaarheid is de mogelijkheid en de wijze om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd.

De gemeente Haarlem hanteert voor deze kwaliteitsaspecten onderstaande normen.

3.4.1.1 Norm voor beschikbaarheid

Het College van B&W en het managementteam zijn van mening dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening voor wat betreft een aantal kritische applicaties wordt gestaakt. Dit geldt onder andere voor de GBA applicatie.
De informatievoorziening rondom Probev moet tijdens de openingstijden van het gemeentehuis, op jaarbasis gemiddeld voor 99,9% beschikbaar zijn.

De openingstijden (voor het publiek) zijn:

maandag tot vrijdag van 09:00 tot 16:00 uur, donderdagavond van 16:00 tot 20:00 uur.

Daarnaast dient de informatievoorziening rondom Probev op jaarbasis tijdens kantooruren voor 99% beschikbaar te zijn.

Als kantooruren worden hier bedoeld:

08:00 -17:00 uur.

Er zijn voldoende voorzieningen getroffen om in geval van calamiteiten na maximaal 2 x 24 uur de dienstverlening aan de burger en aan andere bestuursorganen (waaronder de landelijke afnemers en andere gemeenten die zijn aangesloten op het landelijk GBA-netwerk) te kunnen voortzetten, zie procedure uitwijk.

3.4.1.2 Norm voor integriteit

De technische en organisatorische inrichting van de gemeentelijke informatiesystemen zijn zodanig van aard en opzet dat de gegevens die daarin volledig zijn opgenomen, juist en actueel zijn. De verantwoordelijke personen en afdelingen van de gemeentelijke organisatie van Haarlem hebben hiervoor de nodige maatregelen getroffen.
Het is niet te voorkomen dat gegevens fouten bevatten. Een foutloos bestand met GBA-gegevens is een nobel streven, maar is niet realistisch als concrete eis. Ook binnen de periodieke GBA-audit wordt een foutenmarge geaccepteerd. Als kwaliteitsnorm bij het bepalen van de kwaliteit van de GBA-gegevens wordt door de gemeente Haarlem een foutenpercentage geaccepteerd dat overeenkomt met de normstelling die bij de GBA wordt gehanteerd; te weten de gegevensklassen A, B en C met een foutenpercentage van respectievelijk maximaal 1, 5 en 10%.

3.4.1.3 Norm voor vertrouwelijkheid

Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van de in de diverse registraties opgenomen gegevens. De bevoegdheid van een persoon is afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon, dit ter beoordeling van de informatiebeheerder, op aangeven van de direct leidinggevende van de betreffende medewerker. Alle medewerkers die met GBA gegevens in aanraking komen hebben een geheimhoudingsverklaring ondertekend.

Alle meldingen van verwerkingen van persoonsgegevens die in de zin van de wet GBA en de Wet Bescherming Persoonsgegevens verplicht zijn, zijn door de gemeente Haarlem gedaan aan het College Bescherming Persoonsgegevens in Den Haag.

3.4.1.4 Norm voor controleerbaarheid

Mutaties in persoonsgegevens kunnen verstrekkende gevolgen hebben die ver buiten het domein van de gemeente Haarlem uitkomen. Rechtstreekse toelating tot Nederland is afhankelijk van de nationaliteit. Hoogte en duur van uitkeringen zijn rechtstreeks afhankelijk van leeftijd en burgerlijke staat. De gemeente Haarlem kent dan ook als norm dat 99% van alle mutaties in persoonsgegevens herleidbaar moeten zijn tot een individuele medewerker die hiervoor verantwoordelijk is en dat dit geldt voor 90% van alle raadplegingen.

Samenvatting

Beveiliging van (persoons)gegevens vraagt om een zorgvuldige analyse van de risico's die met de gegevensverwerking samenhangen. Er kunnen verschillende risico's worden genoemd die ertoe kunnen leiden dat het verwerkingsproces stagneert, zoals verlies van gegevens (raakt aan de kwaliteitsaspecten integriteit en beschikbaarheid) en onrechtmatig gebruik van gegevens (raakt aan het aspect vertrouwelijkheid en controleerbaarheid). De in het voorliggend Informatiebeveiligingsplan opgenomen procedures dekken de risico's, behorend bij de aan de verwerking van persoonsgegevens verbonden risicoklasse (II) af.

4 GBA en waardedocumenten

4.1 Inleiding

4.1.1 GBA

Het op schrift stellen van de, in de praktijk van alledag al ingeburgerde, beveiligingsprocedures is noodzakelijk om objectief te kunnen bepalen of de GBA-bestanden en bepaalde processen voldoen aan de eisen ten aanzien van beschikbaarheid (continuïteit), integriteit (betrouwbaarheid), vertrouwelijkheid (exclusiviteit) en controleerbaarheid.

De gemeente moet in het kader van de Wet bescherming persoonsgegevens (WBP) “passende” beveiligingsmaatregelen nemen. In het begrip "passend" ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens.

Naast de Wbp kent de Wet GBA een aantal voorschriften ten aanzien van de beveiliging van de persoonsgegevens. Deze zijn voornamelijk terug te vinden in het Logisch Ontwerp GBA (hoofdstuk 7, Eisen ten aanzien van het beheer).

Naarmate de gegevens een gevoeliger karakter hebben of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekent, worden zwaardere eisen gesteld aan de beveiliging van gegevens.

4.1.2 Reisdocumenten

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

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

4.1.3 Rijbewijzen

Het uitgifteproces van rijbewijzen komt sinds enkele jaren sterk overeen met dat van de Nieuwe Generatie Reisdocumenten. De artikelen 122 tot en met 130 van het Reglement rijbewijzen hebben betrekking op de eisen aan de beveiliging rondom de uitgifte van rijbewijzen. Zo wordt geëist dat de met afgifte van rijbewijzen belaste autoriteiten zorg dragen voor een op schrift gestelde beveiligingsprocedure, met daarin in ieder geval beveiligingsvoorschriften ten aanzien van:

- Toegang van personen tot en het beheer van rijbewijzen;
- De met de afgifte van rijbewijzen verband houdende:
    - Materialen;
    - Apparatuur;
    - Toegangspassen.
- Gebruikerscodes tot de apparatuur;
- De verantwoordelijkheden van de beveiligingsfunctionaris;
- De functiescheiding.

4.2 Periodieke audit, onderzoek en accountantscontrole

4.2.1 GBA

De in het voorliggend Informatiebeveiligingsplan voorgestelde beveiligingsmaatregelen en –procedures vormen voor een groot deel eens in de drie jaar object van onderzoek bij de door het ministerie van Binnenlandse Zaken en Koninkrijkrelaties, agentschap BPR, voorgeschreven GBA-audit. Deze audit, die bestaat uit een controle op de beveiligingsaspecten, op de privacyvoorschriften en een inhoudelijke kwaliteitscontrole, wordt uitgevoerd door een onafhankelijke auditinstelling. Hierbij wordt aangetekend dat bij de GBA-audit niet alleen wordt gekeken naar opzet en bestaan van de maatregelen, maar ook naar de werking die een regelmatige beproeving van de beschreven procedures noodzakelijk maakt. Als norm bij het bepalen van de kwaliteit van de GBA-gegevens wordt bij deze audit het volgende maximale foutenpercentage gehanteerd: in de gegevensklassen A, B en C een foutenpercentage van respectievelijk 1, 5 en 10%.
De uitslag van deze audit wordt door het college van B&W naar het Agentschap BPR gezonden en openbaar gemaakt.

4.2.2 Reisdocumenten

De procedures en maatregelen rondom de beveiliging van reisdocumenten moeten één keer per jaar onderwerp zijn van intern onderzoek met behulp van het zogenaamde 'Beveiligingsnet' (een uitgebreide vragenlijst in de vorm van een 'software-tool'). De resultaten van deze jaarlijkse evaluatie worden gerapporteerd aan de burgemeester. Daarnaast wordt eens in de 3 jaar door een externe deskundige een controle uitgevoerd op de wijze waarop het jaarlijks onderzoek en de jaarlijkse actualisering van het Informatiebeveiligingsplan (onderdeel reisdocumenten) heeft plaatsgevonden. Van deze rapportage van de externe controle wordt een afschrift aan het agentschap BPR gestuurd. De beveiligingsfunctionaris reisdocumenten neemt kennis van zowel de resultaten van het jaarlijkse interne onderzoek als van de resultaten van de driejaarlijkse externe controle en houdt toezicht op de te ondernemen acties op geconstateerde tekortkomingen.

4.2.3 Rijbewijzen

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

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

4.3 Taken, verantwoordelijkheden en bevoegdheden (onderdeel GBA en waardedocumenten).

Op grond van of krachtens de wet GBA, de Paspoortwet en het Reglement Rijbewijzen dienen de taken, verantwoordelijkheden en bevoegdheden van een aantal functionarissen te worden toegekend en vastgelegd. Dit betreft de informatiebeheerder GBA, de gegevensbeheerder GBA, de privacybeheerder GBA, de applicatiebeheerder GBA, de systeembeheerder GBA, beveiligingsfunctionaris reisdocumenten, de Autorisatie Bevoegde Reisdocumenten, de beveiligingsfunctionaris rijbewijzen en de Autorisatie Bevoegde Rijbewijzen. Aan deze eis wordt in dit hoofdstuk voldaan.
Voor alle in dit hoofdstuk voorkomende functies is in de Bijlage Functieverdeling de vervanging vastgelegd.

4.3.1 Verantwoordelijkheden van de informatiebeheerder GBA

De hoofdafdelingsmanager Dienstverlening is aangewezen als informatiebeheerder van het GBA-systeem. Deze zorgt vervolgens voor het toewijzen van taken en verantwoordelijkheden om de hiervoor genoemde vertrouwelijkheid te waarborgen en te controleren.

De informatiebeheerder is manager van het betreffende organisatieonderdeel en bepaalt in het kader van de beveiliging het volgende:

- Het beleid en de keuze rondom de bedrijfsproces ondersteunende applicatie(s) ten behoeve van de GBA;
- Wie de taken van de applicatiebeheerder GBA en de gegevensverwerking GBA uitvoeren;
- Het niveau van autorisatie voor de eindgebruikers voor de GBA applicatie(s);
- Het aan de medewerkers van de afdeling Dienstverlening verlenen van het recht om hun ervaringen rondom aspecten van beveiliging aan de orde te stellen;
- Het onderwerp informatiebeveiliging tenminste eenmaal per jaar te agenderen op het reguliere werkoverleg van de afdeling Dienstverlening;
- Het verplichten van medewerkers van de afdeling Dienstverlening tot het direct melden van onregelmatigheden met betrekking tot de beveiliging;
- Het aanspreken van medewerkers van de afdeling Dienstverlening op geconstateerd onzorgvuldig gedrag in relatie tot beveiliging en het zonodig voorstellen van disciplinaire maatregelen;
- Alle medewerkers van de afdeling Dienstverlening in de gelegenheid stellen om aan relevante trainingscursussen deel te nemen, welke door deskundigen worden verzorgd, een en ander ter bevordering van de beveiligingsbewustwording;
- De gelegenheid bieden aan medewerkers van de afdeling Dienstverlening tot het volgen van cursussen, trainingen en opleidingen in het kader van informatiebeveiliging en dit bevorderen.

De informatiebeheerder GBA kan de uitvoering van hiervoor genoemde taken geheel of gedeeltelijk delegeren aan de daartoe in de Beheerregeling BRP aangewezen medewerkers.

4.3.2 Verantwoordelijkheden van de gegevensbeheerder GBA

De gegevensbeheerder GBA is verantwoordelijk voor:

- De juistheid, actualiteit en betrouwbaarheid van de gegevens die opgenomen zijn of worden in de gemeentelijke basisadministratie persoonsgegevens;
- Het beheer van documentatie op het gebied van de Wet GBA en overige regelgeving op het gebied van de gemeentelijke basisadministratie persoonsgegevens;
- De communicatie met de afnemers en andere houders van gemeentelijke basisadministraties over gegevensverwerking.

De gegevensbeheerder GBA is bevoegd in overleg met de applicatiebeheerder GBA de gegevensverwerkers aanwijzingen te geven betreffende de opname en bijhouding van gegevens in de gemeentelijke basisadministratie persoonsgegevens.

4.3.3 Verantwoordelijkheden van de privacybeheerder GBA

De privacybeheerder GBA is verantwoordelijk voor:

- De inhoudelijke afhandeling van de periodieke gegevensverstrekking die plaatsvindt op basis van een autorisatiebesluit van de Minister van Binnenlandse Zaken Koninkrijksrelaties, evenals de systematische gegevensverstrekking die plaatsvindt op grond van de door het college van burgemeester en wethouders vastgestelde Verordening gemeentelijke basisadministratie persoonsgegevens;
- Het dagelijkse toezicht op de naleving van de privacyvoorschriften die voortvloeien uit de Wet GBA en de Wet bescherming persoonsgegevens met betrekking tot de afdeling Dienstverlening;
- De privacybeheerder GBA voorziet in:
  - De afhandeling van de verzoeken om inzage overeenkomstig artikel 79 van de wet (inzage);
  - De behandeling van alle verzoeken om geheimhouding die op basis van artikel 102 lid 1a ingediend worden en doet eventueel de privacytoets van art. 102 lid 2;

- De afhandeling van verzoeken om inzage in verstrekkingen aan afnemers en derden.

De privacybeheerder GBA is betrokken bij alle bezwaarschriftenprocedures die voortvloeien uit genomen beslissingen op grond van de wet en daarbij behorende regelingen en de Wet bescherming Persoonsgegevens voor zover hierbij privacyaspecten aan de orde zijn.

4.3.4 Verantwoordelijkheden van de applicatiebeheerder GBA

De applicatiebeheerder GBA heeft de volgende taken:

- Verstrekken van adviezen aan de leidinggevende over het te voeren beleid met betrekking tot de GBA applicatie(s);
- Zorg dragen voor de beschikbaarheid en kwaliteit van de GBA applicatie(s);
- Optreden als intermediair tussen gebruikers, het managementoverleg en automatiserings- en informatiedeskundigen met betrekking tot de GBA applicatie(s);
- Signaleren van de behoefte aan uitbreiding van apparatuur en dit overleggen met zowel de gegevensbeheerder GBA als met het hoofd ICT en/of de systeembeheerder;
- Adviseren in geval van daadwerkelijke uitwijk van de GBA applicatie(s);
- Signaleren van het onjuist omgaan met de GBA applicatie(s) en dit melden aan de leidinggevende zodat deze maatregelen kan nemen om dit te voorkomen;
- Zorg dragen voor de tijdige en kwalitatief goede verwerking van gegevens met behulp van de GBA applicatie(s);
- Zorg dragen voor de tijdige en kwalitatief goede oplevering van informatie uit de GBA applicatie(s);
- In samenwerking met afdeling ICT verzorgen van de acceptatie van nieuwe releases van de GBA applicatie(s);
- Bewaken van een juiste toepassing van de gebruikersprocedures ten aanzien van de GBA applicaties;
- Betrokken bij of verzorgen van de training en begeleiding van de medewerkers op het gebied van de GBA applicatie(s);
- Beheren en onderhouden van de bij de GBA applicatie(s) behorende documentatie.

4.3.5 Verantwoordelijkheden van de systeembeheerder GBA

De systeembeheerder is verantwoordelijk voor het technisch onderhoud van de GBA applicatie(s).

De systeembeheerder voorziet in:
- De fysieke beveiliging van de GBA applicatie(s);
- Een dagelijkse back-up die wordt ondergebracht in een daartoe uitgeruste en beveiligde ruimte op een andere locatie dan de ruimte waarin de GBA-apparatuur is opgesteld;
- De technische installatie van gewijzigde of nieuwe versies van de GBA applicatie(s);
- De beschikbaarheid van de GBA applicatie(s) overeenkomstig hetgeen daarover intern en met derden is overeengekomen.

De systeembeheerder is bevoegd:
- Direct maatregelen te treffen als de continuïteit van de GBA applicatie(s) of de daarin opgeslagen informatie acuut in het geding is. Hij is verplicht achteraf ter zake te rapporteren aan de informatiebeheerder;
- Aanwijzingen te geven over:
  - beheer van de GBA applicatie(s);
  - beheer van de bestanden opgenomen in de GBA applicatie(s);
  - reconstructiemaatregelen ten behoeve van de GBA applicatie(s).

4.3.6 Verantwoordelijkheden van de beveiligingsfunctionaris reisdocumenten

Op grond van artikel 93 van de PUN 2001 is door de burgemeester een beveiligingsfunctionaris reisdocumenten aangewezen.

De beveiligingsfunctionaris reisdocumenten is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures die betrekking hebben op de reisdocumenten. De taken en verantwoordelijkheden van deze functionaris zijn in een functiebeschrijving opgenomen.

De beveiligingsfunctionaris reisdocumenten is rechtstreeks verantwoording verschuldigd aan de burgemeester. De beveiligingsfunctionaris reisdocumenten is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van reisdocumenten en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

Van de aanwijzing of de vervanging van de beveiligingsfunctionaris reisdocumenten wordt direct schriftelijk melding gedaan aan het agentschap BPR.

4.3.7 Functiebeschrijving van de beveiligingsfunctionaris reisdocumenten

Plaats in de organisatie

De beveiligingsfunctionaris reisdocumenten wordt conform de PUN 2001 door de burgemeester benoemd. Artikel 93, lid 10 van de PUN bepaalt, dat de functie van beveiligingsfunctionaris niet verenigbaar is met het verrichten van andere handelingen ter uitvoering van de Paspoortwet. De beveiligingsfunctionaris reisdocumenten is rechtstreeks verantwoording verschuldigd aan de burgemeester zonder tussenkomst van de leidinggevenden in de lijn.

Taken

De beveiligingsfunctionaris reisdocumenten is verantwoordelijk voor:

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

Daarnaast is de beveiligingsfunctionaris reisdocumenten voor de volgende algemene beveiligingstaken met betrekking tot reisdocumenten verantwoordelijk:

- Het bewaken van uit te voeren acties voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van het Informatiebeveiligingsplan;
- Het toezicht houden op de actualiteit van het Informatiebeveiligingsplan, de beveiligingsprocessen, -procedures/afspraken en instructies;
- Gevraagd en ongevraagd advies geven aan de burgemeester en het management over verbeteringen ten aanzien van de beveiliging;
- Het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures;
- Het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het tenminste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en –processen;
- Het toezicht houden of (nieuwe) medewerkers worden geïnstrueerd en bekendgemaakt met de beveiligingsprocedures en -processen, betrekking hebbend op de reisdocumenten;
- Het registreren van door de gegevensbeheerder GBA gedane meldingen van beveiligingsincidenten;
- Het rapporteren aan de burgemeester betreffende de stand van zaken van beveiliging, eventueel naar aanleiding van bijzonderheden/incidenten;
- Het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

4.3.8 Verantwoordelijkheden van de Autorisatie Bevoegden Reisdocumenten/Aanvraagstations

De Autorisatie Bevoegde Reisdocumenten/Aanvraagstations is de medewerker die bevoegd is om de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations) te beheren, dat wil zeggen dat hij:

- Autorisaties toekent;
- Autorisaties beëindigt;
- Autorisaties en eventuele wijzigingen daarin aanmeldt bij Morpho;
- Registreert aan wie deze autorisaties zijn verstrekt;
- Toezicht houdt op het zorgvuldig gebruik van deze autorisaties.

De medewerker, die toegang heeft tot het RAAS, ontvangt hiervoor een persoonsgebonden authenticatiekaart in combinatie met een persoonlijke pincode. De medewerker tekent voor ontvangst van de persoonsgebonden authenticatiekaart en bijbehorende pincode. Deze pincode wijzigt de medewerker direct na ontvangst. De autorisatiebevoegde ziet toe op naleving hiervan. De persoonsgebonden authenticatiekaarten en pincodes worden nooit uitgeleend of bekend gemaakt aan anderen.

Persoongebonden authenticatiekaarten worden altijd gescheiden bewaard van de pincodes en opgeborgen in een beveiligde ruimte.

Voor het gebruik van het aanvraagstation wordt de medewerker een gebruikersnaam toegekend en wordt diens vingerafdruk(ken) opgenomen.

De burgemeester wijst per uitgiftelocatie tenminste twee medewerkers aan als Autorisatie Bevoegde Reisdocumenten. De Autorisatie Bevoegde Reisdocumenten legt rechtstreeks verantwoording af aan de burgemeester. Tevens wijst de burgemeester per aanvraagstation tenminste twee medewerkers aan, die zullen functioneren als Autorisatie Bevoegde Aanvraagstation overeenkomstig de gebruikershandleiding bij het aanvraagstation bedoeld in artikel 87 van de PUN.

Omtrent de aanwijzing of vervanging van een Autorisatie Bevoegde Reisdocumenten wordt door de applicatiebeheerder GBA direct melding gedaan aan Morpho.

4.3.9 Verantwoordelijkheden van de beveiligingsfunctionaris rijbewijzen

Op grond van artikel 128, lid 6 van het Reglement Rijbewijzen is door de burgemeester een beveiligingsfunctionaris rijbewijzen aangewezen.

Deze beveiligingsfunctionaris rijbewijzen is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures betrekking hebbend op de rijbewijzen. De taken en verantwoordelijkheden van deze functionaris zijn in een functiebeschrijving opgenomen.

De beveiligingsfunctionaris rijbewijzen is rechtstreeks verantwoording verschuldigd aan de burgemeester. De beveiligingsfunctionaris rijbewijzen is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van rijbewijzen en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

4.3.10 Functiebeschrijving van de beveiligingsfunctionaris rijbewijzen

Plaats in de organisatie

De beveiligingsfunctionaris rijbewijzen is op grond van artikel 128 van het Reglement Rijbewijzen benoemd door de burgemeester. Daarbij is in ieder geval sprake van functiescheiding tussen deze beveiligingsfunctie en de uitvoerende taken met betrekking tot de afgifte en het beheer van rijbewijzen. De beveiligingsfunctionaris rijbewijzen is rechtstreeks verantwoording verschuldigd aan de burgemeester zonder tussenkomst van de leidinggevenden in de lijn.

Taken

De beveiligingsfunctionaris rijbewijzen is verantwoordelijk voor:

- De controle (steekproefsgewijs) op de naleving van de beveiligingsprocessen, -procedures en instructies betreffende rijbewijzen;
- Het (laten) verrichten van onderzoek bij beveiligingsincidenten, met het doel dergelijke situaties in de toekomst te voorkomen;
- Het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten/tekortkomingen in de beveiligingsvoorzieningen.

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

- Het bewaken van uit te voeren acties ter verbetering voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van het Informatiebeveiligingsplan;
- Het toezicht houden op de actualiteit van het Informatiebeveiligingsplan, de beveiligingsprocessen, -procedures/afspraken en instructies;
- Gevraagd en ongevraagd advies geven aan de burgemeester en het management over verbeteringen ten aanzien van beveiliging;
- Het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures;
- Het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het tenminste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en –processen;
- Het toezicht houden of (nieuwe) medewerkers worden geïnstrueerd en bekendgemaakt met de beveiligingsprocedures en -processen, betrekking hebbend op de rijbewijzen;
- Het registreren van door de applicatiebeheerder GBA gedane meldingen van beveiligingsincidenten;
- Het rapporteren aan de burgemeester betreffende de stand van zaken van beveiliging, eventueel naar aanleiding van bijzonderheden/incidenten;
- Het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

4.3.11 Verantwoordelijkheden van de Autorisatie Bevoegde Rijbewijzen

De Autorisatie Bevoegde Rijbewijzen is de medewerker die bevoegd is om de autorisaties voor rijbewijzen te beheren, dat wil zeggen dat hij:

- Autorisaties toekent;
- Autorisaties beëindigt;
- Autorisaties en eventuele wijzigingen daarin aanmeldt bij de RDW;
- Registreert aan wie deze autorisaties zijn verstrekt;
- Toezicht houdt op het zorgvuldig gebruik van deze autorisaties.

De medewerker, die toegang heeft tot het rijbewijzenstation, ontvangt een persoonsgebonden smartcard in combinatie met een persoonlijke pincode. De medewerker tekent voor ontvangst van de persoonsgebonden smartcard en bijbehorende pincode. Deze pincode wijzigt de medewerker direct na ontvangst. De autorisatiebevoegde ziet toe op naleving hiervan. De persoonsgebonden smartcards en pincodes worden nooit uitgeleend of bekend gemaakt aan anderen.
Persoongebonden smartcards worden altijd gescheiden bewaard van de pincodes en opgeborgen in een beveiligde ruimte.

De autorisatiebevoegde draagt zorg voor terugzending van de persoonlijke smartcards, indien deze niet meer worden gebruikt. Deze worden vergezeld van de hiertoe bestemde formulieren teruggestuurd aan de RDW.

De burgemeester wijst per uitgiftelocatie tenminste twee medewerkers aan als Autorisatie Bevoegde Rijbewijzen. De Autorisatie Bevoegde Rijbewijzen legt rechtstreeks verantwoording af aan de burgemeester.

Omtrent de aanwijzing of vervanging van een Autorisatie Bevoegde Rijbewijzen wordt door de applicatiebeheerder GBA direct melding gedaan aan de RDW door middel van het daarvoor bedoelde formulier.

4.4 Functiescheiding ten aanzien van waardedocumenten

Om de kans te verkleinen dat medewerkers van de afdeling Dienstverlening door kwaadwillenden worden misleid (externe fraude) of dat zij al dan niet onder druk van chantage, bedreiging of omkoping misbruik maken van hun bevoegdheden (interne fraude) is functiescheiding bij het verstrekken van waardedocumenten noodzakelijk.

Hieronder een korte uitleg van de relevante termen:

- Aanvraag/verstrekking: Hieronder wordt verstaan het bij de balie behandelen van een aanvraag voor een waardedocument en de beslissing daarop. Bij de aanvraag van een rijbewijs dient een aanvraagformulier te worden ingevuld; bij de aanvraag van een reisdocument moet een foto- en handtekeningformulier worden gebruikt. Eventueel kan daarbij een aanvraagformulier worden ingevuld;
- Beheer: Hieronder wordt verstaan de verantwoordelijkheid voor de materialen en (gepersonaliseerde) waardedocumenten tussen het moment van de aanvraag en de uitreiking;
- Uitreiking: Hieronder wordt verstaan het feitelijk aan de houder ter beschikking stellen van het op zijn naam gestelde waardedocument.

4.4.1 Functiescheiding ten aanzien van reisdocumenten

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

- Tussen de beveiligingsfunctionaris reisdocumenten en degenen die belast zijn met uitvoerende en beheertaken met betrekking tot reisdocumenten (PUN art. 93, lid 10).
  De beveiligingsfunctionaris reisdocumenten mag niet betrokken zijn bij of verantwoordelijkheid dragen voor de procedures rondom reisdocumenten. Dit voorkomt dat de beveiligingsfunctionaris reisdocumenten zijn eigen werk controleert;
- Tussen aanvraag/verstrekking, beheer en uitreiking van reisdocumenten (PUN art. 93 lid 1, sub c). Het reisdocument moet door een andere medewerker worden uitgereikt dan degene die de beslissing op de aanvraag heeft genomen. De functiescheiding op dit gebied wordt in de gemeente Haarlem bereikt doordat op het uitreikformulier of het aanvraagformulier de paraaf van de medewerker is geplaatst, die over de aanvraag heeft beslist. Door de medewerkers wordt er middels de signalering in de reisdocumentenmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt. Voorts dient er ingevolge artikel 93, lid 1, sub c van de PUN functiescheiding te zijn gerealiseerd tussen degene die het beheer heeft over de voorraad gepersonaliseerde reisdocumenten en de medewerkers die de aanvraag behandelen dan wel de uitreiking verzorgen.

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

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

Schriftelijk wordt vastgelegd:

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

De uitdraai uit het RAAS en de afschriften van de in deze periode verstrekte documenten worden afzonderlijk bewaard.
Na afloop van de betreffende periode controleert de beveiligingsfunctionaris reisdocumenten of de schriftelijke vastlegging aanwezig is en de aanvraag/verstrekking, het beheer en de uitreiking op de voorgeschreven wijze hebben plaatsgevonden.

4.4.2 Functiescheiding ten aanzien van rijbewijzen

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

<u>Tussen aanvraag en uitreiking van rijbewijzen</u>
Het rijbewijs wordt door een andere medewerker uitgereikt dan degene die de beslissing op de aanvraag heeft genomen. De functiescheiding op dit gebied wordt in de gemeente Haarlem bereikt doordat op het uitreikformulier of het aanvraagformulier de paraaf van de medewerker is geplaatst,

die over de aanvraag heeft beslist. Door de medewerkers wordt er middels de signalering in de rijbewijsmodule op toegezien dat de uitreiking door een andere medewerker plaatsvindt.
Indien door een te geringe personele capaciteit deze functiescheiding onmogelijk is, kan tijdelijk hiervan worden afgeweken, zie hiervoor de procedure ontbreken van voldoende functiescheiding.

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

Schriftelijk wordt vastgelegd:

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

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

5 Bijlagen

Procedures behorende bij dit Informatiebeveiligingsplan

Procedure Aanvraag en uitreiking waardedocumenten
Procedure Afvoeren van computers
Procedure Antecedentenonderzoek
Procedure Antivirus voorzieningen
Procedure Autorisatie RAAS aanvraagstation
Procedure Autorisatie tot de GBA applicaties
Procedure Back-up en restore RAAS
Procedure Back-up GBA applicatie
Procedure Communicatie over beveiliging
Procedure Correctie
Procedure Gegevensverwerking
Procedure Geheimhouding
Procedure Goedkeuren updates applicatie
Procedure Herstel van mutaties GBA applicatie
Procedure Identificatie en Machtiging
Procedure Introductie nieuw personeel
Procedure Inzagerecht
Procedure Kasbeheer
Procedure Ongedaan maken systematische verstrekkingen
Procedure Ontbreken van voldoende functiescheiding
Procedure Ontvangst en beheer waardedocumenten
Procedure Overvalinstructie en agressief publiek
Procedure Protocollering
Procedure Rapportage van incidenten
Procedure Restore van de GBA applicatie
Procedure Sleutel- en toegangsbeheer
Procedure Sollicitatieonderzoek aanstelling personeel
Procedure Terugmeldingen
Procedure Uitwijk
Procedure Vernietiging van verwijderbare media
Procedure Verstrekken binnengemeentelijk
Procedure Verstrekken buitengemeentelijk
Procedure Verstrekkingen via alternatief medium

Bijlagen behorende bij dit Informatiebeveiligingsplan

Bijlage Aangewezen medewerkers mobiele vingerapparatuur
Bijlage Aangewezen medewerkers waardedocumenten
Bijlage Aangifteformulier overval
Bijlage Activiteitenkalender informatiebeveiliging en privacy
Bijlage Activiteitenkalender waardedocumenten
Bijlage Autorisatiebevoegden waardedocumenten
Bijlage Autorisatieformulier BRP
Bijlage Back-up registratie
Bijlage Beveiligingsdocumentatiedossier
Bijlage Bewerkersovereenkomst
Bijlage Extern onderzoek reisdocumenten
Bijlage Formulier Identificatievragen
Bijlage Formulier Onterechte GBA Verstrekkingen
Bijlage Formulier registratie reconstructie
Bijlage Functieverdeling

Bijlage Geheimhoudingsverklaring
Bijlage intern uitwijkplan GBA
Bijlage Machtiging BZK Bewerker
Bijlage Onderhoudscontract
Bijlage Ontvangstbewijs authenticatiekaart/smartcard
Bijlage Ontvangstlijst waardedocumenten
Bijlage Onvoldoende functiescheiding
Bijlage Parafenlijst inzage
Bijlage Risico-inventarisatie en evaluatie GBA
Bijlage Proces verbaal vernietiging van verwijderbare media
Bijlage Uitdraai Beveiligingsnet
Bijlage Uitwijkcontract
Bijlage Verklarende woordenlijst
Bijlage Verstrekkingentabel GBA
Bijlage Vragenlijst bewerker
Bijlage Werkinstructie back-up RAAS

Rapportages behorende bij dit Informatiebeveiligingsplan

Rapportage Controle autorisaties
Rapportage Controle communicatie over beveiliging
Rapportage Controle gegevensverstrekking en protocollering
Rapportage Controle gegevensverwerking
Rapportage Controle inzagerecht
Rapportage Controle ontbreken van voldoende functiescheiding
Rapportage Controle privacyregelgeving
Rapportage Controle recht op geheimhouding
Rapportage Evaluatie beveiligingsbeleid en plan
Rapportage Evaluatie reisdocumenten
Rapportage Evaluatie rijbewijzen
Rapportage Extern onderzoek reisdocumenten 2007
Rapportage Extern onderzoek reisdocumenten 2010
Rapportage Terugmeldingen
Rapportage Test herstel
Rapportage Test restore
Rapportage Test uitwijk
Rapportage Test verstrekking via alternatief medium

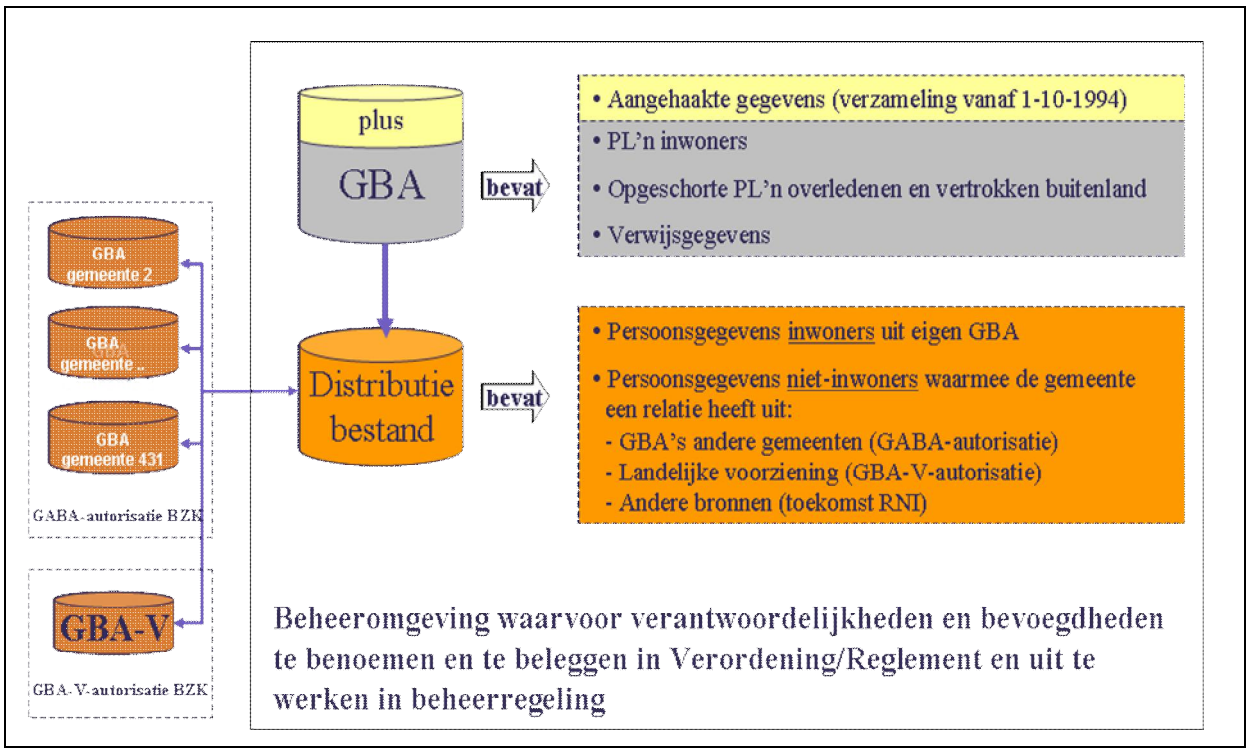
Toelichting op beheerregeling BRP

Inleiding

Sinds 1 januari 2010 geldt voor de hele overheid, en dus ook binnen gemeenten, de verplichting om bij de uitvoering van taken gebruik te maken van persoonsgegevens uit de gemeentelijke basisadministratie persoonsgegevens (GBA). Gemeentelijke afnemers dienen gegevens over de eigen inwoners te betrekken uit de 'eigen basisadministratie'. Gegevens van 'niet-inwoners', die elders in de GBA zijn ingeschreven, moeten afkomstig zijn uit de basisadministraties van die andere gemeenten of uit de landelijke voorziening, de GBA-V.

Het gebruik van persoonsgegevens uit de 'eigen GBA' dient bij of krachtens Verordening te worden geregeld. De verkrijging van gegevens uit de GBA van andere gemeenten is gebaseerd op een autorisatiebesluit van de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

In de praktijk vindt distributie van persoonsgegevens doorgaans niet (meer) rechtstreeks vanuit de GBA plaats, maar vanuit een specifiek daarvoor ingericht distributiebestand. Dat distributiebestand wordt gevoed zowel vanuit de eigen basisadministratie (inwoners) als vanuit de basisadministraties van andere gemeenten (niet-inwoners). In een aantal gevallen worden daar nog persoonsgegevens aan toegevoegd van personen waarmee de gemeente 'een relatie' heeft maar die niet in een basisadministratie zijn opgenomen. Het hiervoor beschrevene wordt geïllustreerd met figuur 1.



Figuur 1: Distributie GBA-gegevens

Beheer

Voor het beheer van de 'eigen GBA' dienen burgemeester en wethouders op grond van artikel 14 van de wet GBA een beheerregeling vast te stellen waarin de hoofdlijnen van het beheer van de basisadministratie is geregeld. De beheerregeling heeft alleen betrekking op het bronbestand, de eigen gemeentelijke basisadministratie.

Het distributiebestand dient echter te worden beschouwd als een technische oplossing (een soort verlengstuk van de GBA), waarop de (privacy)voorschriften van de wet GBA van toepassing zijn en dat, voor wat betreft de persoonsgegevens van de eigen inwoners, valt binnen de reikwijdte van artikel 14 wet GBA.

De beheerregeling is formeel gezien niet van toepassing op de gegevens van de niet-inwoners (welke voornamelijk afkomstig zijn uit de basisadministraties van andere gemeenten dan wel GBA-V). Op dat deel van het distributiebestand is namelijk de Wet bescherming persoonsgegevens (Wbp) van toepassing. De registratie van deze niet-inwoners dient te worden gemeld bij het College bescherming persoonsgegevens (Cbp), maar de Wbp schrijft geen beheerregeling voor.

Desondanks is het van belang om uit oogpunt van eenheid van persoonsinformatie- en privacybeleid en beheersbaarheid van de informatiestromen ook de voor dat deel van het distributiebestand relevante beheeraspecten onder te brengen respectievelijk te integreren in de beheerregeling voor de GBA. Daarmee ontstaat een 'beheerregeling basisregistratie personen' (BRP), bestaande uit de basisadministratie aangevuld met de geautomatiseerde verwerking van persoonsgegevens over personen die niet behoren tot de bevolking van de gemeente.

Verdeling beheerrollen

De beheerregeling onderkent naast een aantal beheerrollen, te weten informatiebeheer, gegevensinhoudelijk beheer, applicatiebeheer, technisch beheer, beveiligingsbeheer en privacybeheer ook de rol van de gegevensverwerker. Gegevensverwerkers verwerken uitsluitend de persoonsgegevens voor de 'eigen basisadministratie'. De inhoudelijke verantwoordelijkheid voor de basisgegevens van personen die niet tot de bevolking van de gemeente worden gerekend, ligt namelijk bij de beheerder van de basisadministratie van de andere gemeenten.

De verdeling van de beheerrollen is mede afhankelijk van de inrichting van de (persoons)informatiehuishouding en het informatiebeleid van de gemeente. De taken, verantwoordelijkheden en bevoegdheden per rol en de bijbehorende competenties zijn richtinggevend voor de plaats in de organisatie waar deze belegd worden.

Privacybeheer

Op de gegevensverwerking over de niet-inwoners is, zoals gemeld, de Wbp van toepassing. Zo is bijvoorbeeld het inzagerecht voor deze categorie van personen gebaseerd op artikel 36 Wet bescherming persoonsgegevens, terwijl de inwoners een beroep kunnen doen op artikel 79 Wet GBA.

De taken van de privacybeheerder zijn in deze beheerregeling verruimd. Verzoeken uit de organisatie om gegevens uit (eigen) basisadministratie(s) of uit de GBA-V dienen door de privacybeheerder getoetst te worden op doelbinding, rechtmatigheid, proportionaliteit, et cetera. De privacybeheerder adviseert de informatiebeheerder, die moet beslissen op dergelijke verzoeken. Een verzoek kan inhouden gebruik te maken van de bestaande ministeriële autorisatie, maar ook uitbreiding van de autorisatie in verband met de uitvoering van een taak die nog niet in het autorisatiebesluit is voorzien.

Artikel 2.

Het betreft hier het functioneel inhoudelijk beheer en het verstrekkingenbeheer van de basisregistratie personen, zoals die is gedefinieerd in artikel 1. De bronhouder beheert inhoud en kwaliteit van de gegevens in de basisadministratie en stelt tevens leveringsvoorwaarden (i.c. privacyvoorwaarden) aan de verstrekking van gegevens uit de basisadministratie.

De gegevensverstrekking binnen de gemeentelijke organisatie over niet-inwoners uit basisadministraties van andere gemeenten, dient gebaseerd te zijn op het autorisatiebesluit van de minister van Binnenlandse Zaken. Het beheer en de uitvoering van dat autorisatiebesluit, maken deel uit van het functioneel inhoudelijk en verstrekkingenbeheer van de basisregistratie personen.

De hier beschreven beheerrol is belegd bij de hoofdafdelingsmanager Dienstverlening. Van belang is hierbij op te merken dat voor de verstrekking van gegevens aan de binnengemeentelijke gebruikers, gebruik gemaakt wordt van het datadistributiesysteem/basisregistratiesysteem waarvan het beheer niet bij de bronhouder is belegd, maar bij het hoofd ICT Het betreft hier een soort gegevensmagazijn, waar de BRP deel van uitmaakt. Hoewel in hiërarchische zin niet verantwoordelijk voor deze oplossing, blijft de hoofdafdelingsmanager Dienstverlening wel functioneel inhoudelijk verantwoordelijk. De functionaris bij afdeling ICT die belast is met de verstrekking van gegevens uit de BRP ontvangt functioneel inhoudelijke sturing van de hoofdafdelingsmanager Dienstverlening.

Beheerregeling gemeentelijke basisregistratie personen[1]

Burgemeester en wethouders van de gemeente Haarlem,

Gelet op de
Wet gemeentelijke basisadministratie persoonsgegevens;
Wet bescherming persoonsgegevens

Besluiten:

Vast te stellen de navolgende beheerregeling gemeentelijke basisregistratie personen gemeente Haarlem:

[1] waarin geïncorporeerd de wettelijke verplichte beheerregeling ingevolge artikel 14 van de wet GBA

Hoofdstuk 1 ALGEMENE BEPALINGEN

Artikel 1 Begripsbepalingen

Deze regeling verstaat onder:

a.	de wet:	de Wet gemeentelijke basisadministratie persoonsgegevens (Stb. 1994, 494);
b.	besluit:	het Besluit gemeentelijke basisadministratie persoonsgegevens
c.	verantwoordelijke:	het college van burgemeester en wethouders dat via de wet is aangewezen als verantwoordelijke;
d.	basisadministratie:	de geautomatiseerde verwerking van persoonsgegevens over de bevolking van de gemeente Haarlem als bedoeld in artikel 2 van de wet;
e.	basisregistratie personen:	de basisadministratie aangevuld met de geautomatiseerde verwerking van persoonsgegevens over personen die niet behoren tot de bevolking van de gemeente Haarlem;
f.	ingeschrevene:	degene ten aanzien van wie een persoonslijst als bedoeld in artikel 1 van de wet GBA, in de basisadministratie is opgenomen;
g.	GBA-V:	de verstrekkingsvoorziening als bedoeld in artikel 66a van het besluit;
h.	autorisatiebesluit:	een besluit als bedoeld in artikel 91, eerste lid, van de wet betreffende de systematische verstrekking van persoonsgegevens uit de GBA-V of uit de basisadministraties van andere gemeenten;
i.	beheerder:	de functionaris die namens de verantwoordelijke is belast met de dagelijkse zorg voor de basisregistratie personen en het beheer van het autorisatiebesluit;
j.	Informatiebeheer:	het geheel van activiteiten gericht op beleidsvoorbereiding ter zake de basisregistratie personen, de ontwikkeling van kwaliteitsprocedures, beveiligingsprocedures, verstrekking- en privacyprocedures, evenals de coördinatie bij de uitvoering van deze procedures;
k.	beveiligingsbeheer:	het geheel van activiteiten gericht op het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Informatiebeveiligingsplan;
l.	gegevensbeheer:	het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening;
m.	systeembeheer:	het geheel van activiteiten gericht op het onderhouden van de technische aspecten van het toepassingsysteem;
n.	applicatiebeheer:	het geheel van activiteiten gericht op het ondersteunen van het GBA-toepassings- systeem en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening;
o.	privacybeheer:	het geheel van activiteiten gericht op de bescherming van de persoonlijke levenssfeer bij het verzamelen en verwerken van persoonsgegevens in de basisregistratie personen en de informatievoorziening daaruit;
p.	gegevensverwerking:	het ontlenen van gegevens aan documenten en deze op een voorgeschreven wijze middels het daartoe bestemde toepassingssys-teem opnemen in een gegevensbestand;

Artikel 2

1. De hoofdafdelingsmanager Dienstverlening is beheerder van de basisregistratie personen en van het autorisatiebesluit en in die hoedanigheid informatiebeheerder en privacybeheerder. Hij kan de taak van informatiebeheerder en privacybeheerder geheel of gedeeltelijk mandateren aan een of meer ondergeschikte ambtenaren.

2. De security-officer is beveiligingsbeheerder. De beveiligingsbeheerder is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortvloeien uit het Informatiebeveiligingsplan.

3. De beveiligingsbeheerder rapporteert periodiek (minimaal eens per jaar) aan het managementteam en het College van B&W.

Artikel 3

1. De informatiebeheerder wijst functionarissen aan die worden belast met:
   a) gegevensbeheer;
   b) applicatiebeheer;
   c) privacybeheer
   d) gegevensverwerking;
   e) het namens het college van burgemeester en wethouders afnemen van de in artikel 36, lid 2, onder sub e, van de wet bedoelde verklaring.

2. Het college van Burgemeester en wethouders wijst medewerkers aan die zijn belast met het systeembeheer en het beveiligingsbeheer.

Hoofdstuk 2 HET INFORMATIEBEHEER

Artikel 4

De informatiebeheerder voorziet in:
a) een jaarlijkse planning van de beheeractiviteiten;
b) een jaarlijkse rapportage aan het college van burgemeester en wethouders over de bij a. bedoelde planning, waarbij tevens inzicht wordt gegeven in de kengetallen van de bijhoudings- en beheerprocedures;
c) een jaarlijkse rapportage over de resultaten die voortvloeien uit de in artikel 12 bedoelde kwaliteitssteekproef;
d) administratieve beheerprocedures, voor zover hier niet door of bij de wet in is voorzien;
e) periodiek overleg tussen hem en de op basis van de beheerregeling aangewezen beheerders;
f) richtlijnen voor de bijhouding van de basisregistratie personen.

Artikel 5

De informatiebeheerder adviseert het college van burgemeester en wethouders over de navolgende aspecten die voortvloeien uit deze basisregistratie te weten:
a) persoonsinformatievoorziening;
b) beveiliging;
c) privacy;
d) gegevenskwaliteit;
e) personeelsaangelegenheden.

Artikel 6

De informatiebeheerder beslist:

a) over de installatie van nieuwe of gewijzigde versies van het GBA-toepassingssysteem;
b) op verzoeken van binnengemeentelijke afnemers tot rechtstreekse toegang tot de basisregistratie personen en de GBA-V;
c) op verzoeken van binnengemeentelijke afnemers en derden tot het verkrijgen van gegevens uit de basisregistratie personen;
d) op verzoeken van binnengemeentelijke afnemers tot het systematisch[2] verkrijgen van gegevens;
e) over het toekennen van autorisaties met betrekking tot het bepaalde in dit artikel, onder b, c en d.

Artikel 7

De informatiebeheerder ziet er op toe dat:

a) de in deze regeling opgenomen bepalingen worden nageleefd;
b) de behandeling en afhandeling van verzoeken om gegevensverstrekking als genoemd in artikel 6 geschiedt volgens de bepalingen uit de wet, de Verordening basisregistratie personen en Wet bescherming persoonsgegevens;
c) de bij of krachtens de wet opgelegde verplichtingen ten aanzien van inrichting en bijhouding, evenals de beveiliging van de basisregistratie personen worden nageleefd;
d) dat alle in artikel 3, lid 1 genoemde functionarissen, alsmede de systeembeheerder op de hoogte zijn van de installatie van nieuwe of gewijzigde versies van het GBA-toepassingsysteem en van de gevolgen van deze installatie;
e) de beveiligingsvoorschriften die voortvloeien uit het Informatiebeveiligingsplan worden nageleefd.

Artikel 8

De informatiebeheerder, of een op grond van artikel 3, lid 1 aangewezen functionaris, neemt deel aan buitengemeentelijk overleg betreffende onderwerpen die het beheer van de basisregistratie personen aangaan.

Hoofdstuk 3 HET GEGEVENSBEHEER

Artikel 9

1. De gegevensbeheerder is verantwoordelijk voor:
   a) de juistheid, actualiteit en betrouwbaarheid van de gegevens die opgenomen zijn of worden in de basisadministratie[3];
   b) het beheer van documentatie op het gebied van de wet en overige regelgeving op het gebied van de basisadministratie;
   c) de communicatie met de afnemers en andere houders van basisadministraties over gegevensverwerking;
   d) het verwerken van complexe mutaties en correcties met betrekking tot de basisadministratie;

[2] onder systematische verkrijging wordt hier verstaan de spontane verstrekking van mutaties op gegevens, hetzij elektronisch hetzij op papier (mutatieberichtgeving).
[3] Het betreft hier de basisadministratie.

e) het uitzetten van richtlijnen met betrekking tot het actualiseren en corrigeren van persoonsgegevens in de basisadministratie.

2. De gegevensbeheerder beslist binnen 5 werkdagen op het in behandeling nemen van een melding van een afnemer die gerede twijfel heeft over de juistheid van een in de basisadministratie opgenomen (authentiek) gegeven en stelt de afnemer in kennis van deze beslissing.

Artikel 10

De gegevensbeheerder voorziet in:

a) de behandeling van wijzigingsverzoeken als bedoeld in artikel 81, 82 en 83 van de wet;
b) controlewerkzaamheden ter waarborging van de kwaliteit van de basisregistratie personen.

Artikel 11

De gegevensbeheerder is bevoegd, in overleg met de applicatiebeheerder, vanuit de in artikel 9 bedoelde verantwoordelijkheid de gegevensverwerkers aanwijzingen te geven betreffende de opname en bijhouding van gegevens in de basisadministratie.

Artikel 12

Periodiek wordt de inhoudelijke kwaliteit van het bestand van persoonslijsten in de basisadministratie onderworpen aan een audit door een namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen auditinstelling.
De gegevensbeheerder voorziet in een doorlopende kwaliteitssteekproef en de uitvoering van de daarmee samenhangende verbetermaatregelen gericht op het welslagen van de eerder vermelde audit.

Artikel 13

De gegevensbeheerder neemt deel aan het in artikel 4, onder e genoemde overleg.

Hoofdstuk 4 HET SYSTEEMBEHEER

Artikel 14

De systeembeheerder is verantwoordelijk voor het technisch onderhoud van het toepassingssysteem.

Artikel 15

De systeembeheerder voorziet in:

a) de fysieke beveiliging van het toepassingssysteem;
b) een dagelijkse back-up die wordt ondergebracht in een daartoe uitgeruste en beveiligde ruimte op een andere locatie dan de ruimte waarin de GBA-apparatuur is opgesteld;
c) de technische installatie van gewijzigde of nieuwe versies van het toepassingssysteem;
d) de beschikbaarheid van het toepassingssysteem overeenkomstig hetgeen daarover intern en met derden is overeengekomen.

Artikel 16

De systeembeheerder is bevoegd:
a) direct maatregelen te treffen wanneer de continuïteit van het toepassingssysteem of de daarin opgeslagen informatie acuut in het geding is; hij is verplicht achteraf ter zake te rapporteren aan de informatiebeheerder;
b) aanwijzingen te geven over:
    - beheer toepassingssystemen;
    - beheer van bestanden;
    - reconstructiemaatregelen.

Artikel 17

De systeembeheerder neemt deel aan het in artikel 4, onder e genoemde overleg.

Hoofdstuk 5 HET APPLICATIEBEHEER

Artikel 18

De applicatiebeheerder voorziet in:
a) een planning van periodieke gegevensverstrekkingen die op basis van het autorisatiebesluit wordt gedaan;
b) de communicatie bij storingen in hard- en software;
c) een logboek waarin bijzondere gebeurtenissen worden bijgehouden;
d) de toekenning van de autorisatieniveaus voor actualiseringen aan de gegevensverwerkers, de gegevensbeheerder, de applicatiebeheerder en de informatiebeheerder op grond van een besluit van de informatiebeheerder;
e) de bijhouding van een dossier van de autorisaties, die overeenkomstig artikel 6 door de informatiebeheerder zijn toegekend;
f) het testen en evalueren van nieuwe versies van het toepassingssysteem, alsmede het testen en evalueren van nieuwe apparatuur;
g) de beoordeling van de gevolgen van de installatie van nieuwe en of gewijzigde versies van het toepassingssysteem;
h) de bijhouding van een verzameling van alle problemen en klachten, die bij het gebruik van het toepassingssysteem ontstaan;
i) een oplossing, eventueel door inschakeling van de systeembeheerder of een derde, voor de onder h genoemde problemen en klachten;
j) de voorlichting aan de alle in artikel 3 genoemde functionarissen met betrekking tot de gevolgen van een nieuwe of gewijzigde versie van het toepassingssysteem;
k) de coördinatie van de werkzaamheden in geval van uitwijk in overleg met de systeembeheerder;
l) de vormgeving en inhoud van documenten, die rechtstreeks aan de basisregistratie personen worden ontleend;
m) de afhandeling van verzoeken omtrent managementgegevens;
n) een zo spoedig mogelijke oplossing in geval van storingen binnen het toepassingssysteem, zonodig door inschakeling van een derde.

Artikel 19

De applicatiebeheerder is verantwoordelijk voor:
a) de ondersteuning bij het gebruik van het toepassingssysteem;
b) het tijdig opschonen van de relevante bestanden in de database;

c) de technische afhandeling van de periodieke gegevensverstrekking die plaatsvindt op basis van een autorisatiebesluit, alsmede de systematische gegevensverstrekking die plaatsvindt op basis van de door het college van burgemeester en wethouders vastgestelde procedurebeschrijving voor de basisregistratie personen;
d) het beheer van de tabellen van de basisregistratie personen;
e) het beheer van de gebruikersdocumentatie.

Artikel 20

De applicatiebeheerder is bevoegd:
a) gegevensverwerkers en het personeel van externe afdelingen/diensten die direct toegang hebben tot de basisregistratie personen aanwijzingen te geven over het gebruik van het toepassingssysteem;
b) over het gebruik van de basisregistratie personen gedragsregels op te stellen.

Artikel 21

De applicatiebeheerder is verantwoordelijk voor de gehele of gedeeltelijke uitvoering van de uitwijkprocessen zoals beschreven in de procedure uitwijk.

Artikel 22

De applicatiebeheerder ziet erop toe dat voorgeschreven procedures uit het Informatiebeveiligingsplan worden nageleefd.

Artikel 23

De applicatiebeheerder neemt deel aan:
a) het overleg genoemd in artikel 4, onder e;
b) het externe gebruikersoverleg.

Hoofdstuk 6 HET PRIVACYBEHEER

Artikel 24

De privacybeheerder is verantwoordelijk voor:

a) de inhoudelijke afhandeling van de verzoeken als bedoeld in artikel 6, onder b, c en d van deze beheerregeling;
b) het dagelijkse toezicht op de naleving van de privacyvoorschriften die voortvloeien uit de wet en de Wet bescherming persoonsgegevens.

Artikel 25

De privacybeheerder voorziet in:

a) de afhandeling van de verzoeken om inzage in de basisregistratie personen overeenkomstig artikel 79 van de wet respectievelijk artikel 35 van de Wet bescherming persoonsgegevens (inzage);
b) de behandeling van alle verzoeken om geheimhouding die op basis van artikel 102 lid 1 van de wet ingediend worden en de eventuele privacytoets als bedoeld in artikel 102 lid 2 van de wet;
c) de afhandeling van verzoeken ingevolge de artikelen 36, 37 en 40 van de Wet bescherming persoonsgegevens;
d) de kennisgeving ingevolge artikel 38 van de Wet bescherming persoonsgegevens;
e) de afhandeling van verzoeken om inzage in verstrekkingen uit de basisadministratie aan afnemers en derden.

Artikel 26

De privacybeheerder is bevoegd:

a) op grond van het in artikel 24, sub b genoemde toezicht, alle gebruikers van het toepassingssysteem aanwijzingen te geven;
b) ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de basisregistratie personen, waarbij de persoonlijke levenssfeer in het geding is.

Artikel 27

De privacybeheerder is betrokken bij alle bezwaarschriftenprocedures die voortvloeien uit genomen beslissingen op grond van de wet en daarbij behorende regelingen, de Wet bescherming persoonsgegevens voor zover hierbij privacyaspecten aan de orde zijn.

Hoofdstuk 7 DE GEGEVENSVERWERKING

Artikel 28

De gegevensverwerkers voorzien in:

a) het verwerken van de gegevens in de basisadministratie overeenkomstig de voorschriften van de krachtens de wet voorgeschreven systeembeschrijving (Logisch Ontwerp GBA) en de handleiding uitvoeringsprocedures, voor zover daartoe door de applicatiebeheerder geautoriseerd;
b) het verzamelen van de daarvoor bestemde gegevens;
c) de archivering van de brondocumenten op grond waarvan de gegevens zijn verwerkt;
d) de behandeling van mutaties;
e) de behandeling van het netwerkverkeer, behalve de periodieke gegevensverstrekking;
f) de behandeling van de foutverslagen, voortvloeiend uit de inkomende netwerk-berichten;
g) de toetsing van de waarde die aan overgelegde brondocumenten kan worden toegekend aan de hand van artikel 36 van de wet en ziet erop toe dat geen gegevens worden verwerkt uit documenten waaraan bij of krachtens de Wet geen ontleningstatus is gegeven;
h) de dagelijkse controle van de in de basisadministratie aangebrachte actualiseringen;
i) de kennisgeving aan de ingeschrevene voor wat betreft de verwerking van:
   - wijziging van het naamgebruik;
   - vervolginschrijving voor zover het betreft een binnengemeentelijke verhuizing en een vervolginschrijving die leidt tot opname in de basisadministratie;
j) de toezending van de complete persoonslijst aan de ingeschrevene ingeval van een:
   - 1e inschrijving in de basisadministratie;
   - een vervolginschrijving uit het buitenland.

Artikel 29

De gegevensverwerkers:

a) beslissen op aangiften en verzoekschriften die op grond van de wet worden gedaan met inachtneming van het gestelde in artikel 24 en voor zover hier niet op andere wijze in is voorzien;
b) beslissen over het verwerken van resultaten van onderzoeken die zijn ingesteld naar aanleiding van een melding van een afnemer;
c) stellen afnemers in kennis van de beslissing ingevolge sub b van dit artikel.

Hoofdstuk 8 HET BEVEILIGINGSBEHEER

Artikel 30

De beveiligingsbeheerder is verantwoordelijk voor het toezicht op naleving van de beveiligings-maatregelen en –procedures zoals uitgewerkt in het Informatiebeveiligingsplan.

Artikel 31

De beveiligingsbeheerder is bevoegd om het management van de afdeling Dienstverlening adviezen te geven ten aanzien van beveiligingsvoorschriften, die voortvloeien uit de wet en het Informatiebeveiligingsplan.

Artikel 32

De beveiligingsbeheerder ziet er op toe dat:
a) beveiligingsvoorschriften die voortvloeien uit de wet en het Informatiebeveiligingsplan worden nageleefd;
b) de in deze regeling opgenomen bepalingen inzake beveiliging worden nageleefd.

Artikel 33

De beveiligingsbeheerder adviseert rechtstreeks aan het college van burgemeester en wethouders over beveiligingsaspecten die uit het Informatiebeveiligingsplan voortvloeien.

Artikel 34

De beveiligingsbeheerder voorziet in een jaarlijks verslag over de activiteiten inzake het Beveiligingsbeheer.

Hoofdstuk 9 SLOTBEPALINGEN

Artikel 35

De in deze regeling opgenomen bepalingen gelden voor de basisregistratie personen als bedoeld artikel 1 van de Verordening Basisregistratie Personen evenals voor de daarin genoemde aangehaakte gegevens.

Artikel 36

Deze regeling treedt in werking op de eerste dag na die waarop zij is bekend gemaakt.
De Beheerregeling GBA zoals vastgesteld door het college van burgemeester en wethouders van de gemeente Haarlem op 12 januari 2010 wordt hiermee ingetrokken.

Artikel 37

Deze regeling wordt aangehaald als Beheerregeling gemeentelijke basisregistratie personen gemeente Haarlem.

Aldus besloten in de vergadering van het college van burgemeester en wethouders van 22 januari 2013.

Burgemeester en wethouders van Haarlem.

De secretaris, de heer J. Scholten

De burgemeester, de heer B. Schneiders

Bijlage 1: Aanwijzing van beheerfunctionarissen

Op grond van artikel 3, lid 1 van de Beheerregeling basisregistratie personen zijn de navolgende beheerfunctionarissen aangewezen:

Gegevensbeheer

Als gegevensbeheerder is aangewezen de heer A.G.H.P. Jonkers, gegevensbeheerder GBA.
Zijn plaatsvervanger is mevrouw S.W. Snoeks, applicatiebeheerder.

Applicatiebeheer

Als applicatiebeheerder is aangewezen mevrouw S.W. Snoeks, applicatiebeheerder.
Haar plaatsvervanger is mevrouw M. Blauwhof-van der Goes, aplicatiebeheerder.

Naast de gegevensbeheerder zijn tevens belast met het berichtenverkeer:

- mevrouw S.W. Snoeks, applicatiebeheerder.
- mevrouw M. Blauwhof-van der Goes, applicatiebeheerder.

Privacybeheer

Als privacybeheerder is aangewezen mevrouw E.R. van Agteren-de Haan.
Haar plaatsvervanger is mevrouw J. Korsaan.

Gegevensverwerking

Als gegevensverwerkers worden alle medewerkers van de hoofdafdeling Dienstverlening aangewezen.

Afnemen verklaringen artikel 36, lid 2 van de wet.

De bevoegdheid tot het namens het college van burgemeester en wethouders afnemen van de in artikel 36, lid 2, onder sub e, van de wet bedoelde verklaring wordt toegekend aan:

- Mevrouw R. Hellingman
- De heer D.W. van den Eijkhof
- Mevrouw H.J. Kooijman
- De heer L.P. Kossen
- De heer F. Oonk
- Mevrouw Y.J.M. Pijnaker
- Mevrouw D.P. Suriel-Lewis
- Mevrouw S.M. Swart-Stokman
- Mevrouw I.H.J. Voogd-Smit

Haarlem, 15 januari 2013

de hoofdafdelingsmanager Dienstverlening
mevrouw H.M. Agterhuis

Op grond van artikel 3, lid 2 van de Beheerregeling basisregistratie personen zijn de navolgende beheerfunctionarissen aangewezen:

Beveiligingsbeheer

Als beveiligingsbeheerder is aangewezen mevrouw E. Sebok
Als haar plaatsvervanger is aangewezen de heer M.J. Caspers

Systeembeheer

Als systeembeheerder is aangewezen de heer R.G. Evers.
Als zijn plaatsvervanger is aangewezen de heer E. Boogaard.

Burgemeester en wethouders van Haarlem, 22 januari 2013

De secretaris, de heer J. Scholten

De burgemeester, de heer B. Schneiders

Privacyreglement BRP

Toelichting op het privacyreglement BRP van de gemeente Haarlem

Dit reglement vloeit voort uit de Verordening gemeentelijke basisregistratie personen (BRP). De verordening omvat het bestuurlijk-juridisch kader voor de persoonsinformatiehuishouding met ingang van 1 januari 2010. De raad heeft de nadere regeling van verantwoordelijkheid, beheer en gegevensverwerking opgedragen aan het college van burgemeester en wethouders in hun rol als verantwoordelijke voor de verwerking van persoonsgegevens in de BRP. Hieronder volgt voor zover nodig een nadere toelichting op de artikelen in dit reglement.

Artikel 1. Begripsbepalingen

Basisadministratie en basisregistratie personen

In dit artikel worden de begripsbepalingen uitgewerkt. Het reglement betreft de basisregistratie personen. Dat is een combinatie van de basisadministratie, waarin persoonsgegevens van personen die in gemeente Haarlem woonachtig zijn en de registratie van gegevens van niet-inwoners. Om over de gegevens van niet-inwoners te kunnen beschikken is (voor zover van de niet-inwoner in de GBA een persoonslijst is opgenomen) een besluit van de minister van Binnenlandse Zaken nodig, het onder g in dit artikel genoemde autorisatiebesluit.
De basisregistratie bevat naast gegevens van inwoners en niet-inwoners de zogenaamde aangehaakte gegevens. Dat zijn gegevens van voormalige inwoners (aangehaakte gegevens hebben toch ook betrekking op actuele inwoners?) van gemeente Haarlem, die nog in gebruik zijn, maar die strikt formeel geredeneerd niet tot de basisadministratie worden gerekend. Deze gegevens maken geen deel uit van het gegevenspakket van de basisadministratie.

Authentieke gegevens

Sinds 1 januari 2010 dienen overheidsorganisaties en dus ook gemeenten bij de verwerking van persoonsgegevens voor publiekrechtelijke taken gebruik te maken van de authentieke gegevens uit de basisadministraties. Authentieke gegevens zijn gegevens die als zodanig door de wet worden aangemerkt. In de memorie van toelichting op het wetsvoorstel wordt het begrip authentiek gegeven als volgt omschreven: “Authentieke gegevens zijn, gezien het geheel van wettelijke taken, voor alle overheidsinstanties vitaal of veelvuldig en om uiteenlopende redenen nodig, kwalitatief hoogwaardig en als zodanig bij of krachtens de wet aangewezen”. De mate van zekerheid en dus de bewijskracht die aan een gegeven in de GBA kan worden toegekend wordt bepaald door de brondocumenten waaraan ze zijn ontleend. Welke gegevens tot de authentieke gegevens worden gerekend is vastgelegd in bijlage 1d behorende bij artikel 58a van het Besluit GBA.

Artikel 2. Beheer

Het beheer van de basisregistratie personen is belegd bij de hoofdafdelingsmanager Dienstverlening.

Artikel 3. Authentieke gegevens

Afnemers zijn ingevolge artikel 3b Wet GBA verplicht om authentieke gegevens te gebruiken bij vervulling van wettelijke taken en ingevolge artikel 62 wet GBA bij gerede twijfel aan het authentieke gegeven dit terug te melden aan de bronhouder.

Artikel 4. Rechtstreekse toegang tot de basisregistratie personen en de GBA-V

Rechtstreekse toegang wil zeggen: het via een "on-line verbinding" kunnen raadplegen of muteren van gegevens, zonder tussenkomst van anderen. Lid 1, sub a regelt de toegang van de beheerder en de medewerkers bij de afdelingen die uitvoering geven aan de Wet GBA. Lid 1, sub b heeft betrekking op de toegang door een bewerker.

Behalve de reguliere afdelingen van een gemeente, zoals belastingen of Sociale Zaken, heeft het regionale politiekorps op dezelfde wijze toegang tot de GBA. Dit is geregeld in artikel 96, tweede lid van de Wet GBA.

Artikel 5. Verstrekking van gegevens aan binnengemeentelijke afnemers

Er zijn binnengemeentelijke afnemers aan wie systematisch gegevens worden verstrekt zonder dat

hun rechtstreekse toegang tot de basisregistratie personen is gegeven. In dit verband kan worden gedacht aan periodieke selecties en mutatieberichtgeving.

Artikel 6. Verbanden met andere registraties

Op grond van dit artikel vindt verstrekking van persoonsgegevens uit de basisregistratie personen aan andere binnengemeentelijke afdelingen plaats. Het aanleggen van verbanden hangt samen met het gemeentelijk informatiebeleid. De Wet GBA verplicht in artikel 96 tot het benoemen van de verbanden die in de gemeente zijn aangelegd tussen de verschillende administraties. Een voorbeeld van een dergelijk verband is die van de integratie van de basisadministratie in de basisregistratie. Aangegeven moet worden welke registraties het betreft, waarvoor de gegevens worden gekoppeld, om welke afdeling het gaat en door wie de gegevens worden beheerd.

Artikel 7. Overige verstrekkingen

Gemeenten hebben de bevoegdheid om op basis van artikel 100 van de Wet GBA bij of krachtens verordening te bepalen of en in welke mate gegevens worden verstrekt uit de basisadministratie aan zogenaamde vrije derden.

Voorwaarde is dat het gemeentelijk verstrekkingenbeleid is vastgelegd bij of krachtens een gemeentelijke verordening. Met de wijziging van artikel 100 van de wet GBA per 1 september 2001 heeft de wetgever de categorie van personen en instellingen die de gemeente van gegevens kan voorzien aanzienlijk beperkt.

Het verstrekken van gegevens aan commerciële bedrijven behoort niet tot het doel van de GBA en staat in beginsel op gespannen voet met de primaire doelstelling van de basisadministraties. Om die reden wordt gegevensverstrekking op grond van artikel 100 aan commerciële instellingen en bedrijven volledig uitgesloten. Commerciële instellingen zoals incassobureaus en postorderbedrijven hebben dus geen recht op gegevensverstrekking.

Ook de categorie van gegevens die mogen worden verstrekt, is verder afgebakend. Alleen de in artikel 100, tweede lid Wet GBA vermelde gegevens mogen worden verstrekt. Ingevolge artikel 102 van de Wet GBA heeft de burger het recht geheimhouding tot verstrekking van zijn gegevens te vragen. In dat geval wordt de gevraagde informatie niet verstrekt.

Onder artikel 100 Wet GBA is gegevensverstrekking alleen mogelijk aan rechtspersonen zonder winstoogmerk voor zover de verstrekking noodzakelijk is in het belang van betrokkenen of van de rechten en vrijheden van anderen. Daarbij wordt nagegaan of de verstrekking wordt gerechtvaardigd door een dringende maatschappelijke behoefte, een gemeentelijk belang, of de verstrekking in de juiste verhouding staat tot het doel waarvoor de gegevens worden gevraagd en of dit doel op een minder ingrijpende wijze kan worden bereikt.

Een voorbeeld van gegevensverstrekkingen aan rechtspersonen is de verstrekking van gegevens aan woningcorporaties in het kader van de samenwerking op het gebied van de fraudebestrijding en eerlijke verdeling van de woonruimte.

Aan particulieren mogen gegevens worden verstrekt ten behoeve van een persoonlijk niet-commercieel belang zoals in verband met een reünie of opsporing van een familielid. Verplicht is gesteld dat de gemeente eerst uitdrukkelijk toestemming verkrijgt van de ingeschrevene van wie de gegevens worden verstrekt. De schriftelijke toestemmingen moeten een jaar lang worden bewaard. Daarnaast moeten informatieverstrekkingen die plaatsvinden op basis van artikel 100 worden geprotocolleerd (artikel 9).

Artikel 8. Terugmeldplicht

Dit artikel regelt de verplichting van bestuursorganen om bij gerede twijfel aan de juistheid van de authentieke gegevens terug te melden aan de beheerder van de basisadministratie. Gegevensuitwisselingen beperken zich in het algemeen niet uitsluitend tot de authentieke gegevens. Ook in de niet-authentieke gegevens kunnen eventuele fouten voorkomen, die door daartoe door het college aan te wijzen afnemers teruggemeld moeten kunnen worden.

Op grond van artikel 62, vierde lid, van de wet GBA is het college van burgemeester en wethouders de bevoegdheid toegekend om:

- nadere regels te stellen omtrent de terugmelding door de binnengemeentelijke afnemers aan de basisadministratie;
- nadere regels te stellen omtrent de kennisgeving door het college aan de binnengemeentelijke afnemer naar aanleiding van een terugmelding;
- binnengemeentelijke afnemers aan te wijzen die een terugmelding doen op andere dan de authentieke gegevens, waarbij is aangegeven welke gegevens dit betreft.

De 'terugmelding aan de basisadministratie' houdt zowel terugmelding in aan de eigen basisadministratie van de gemeente Haarlem als ook aan de basisadministraties van de andere gemeenten.

Artikelen 9 tot en met 12 Rechten van de burger

De wet GBA regelt uitputtend de rechten van de burger met betrekking tot inzage, correctie en verwijdering van diens gegevens in de basisadministratie. Op het deel van de basisregistratie dat niet als basisadministratie wordt aangemerkt, is de Wet bescherming persoonsgegevens van toepassing. De rechten die de burger op grond van die wet heeft, zijn overgenomen in dit reglement.

Artikel 13. Beveiliging

De GBA stelt een aantal eisen op het gebied van beveiliging:
Artikel 31 Besluit GBA stelt dat er voldoende voorzieningen van technische en organisatorische aard getroffen moeten zijn ter beveiliging van de in de GBA vermelde gegevens tegen verlies of aantasting van deze gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking van deze gegevens.

Het daarin gestelde is uit te splitsen naar de volgende aandachtsgebieden:

- Het systeem dan wel de methode voor het ontwikkelen, uitvoeren, meten dan wel controleren en bijsturen van beveiligingsmaatregelen;
- de maatregelen van technische aard om verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking van deze gegevens te voorkomen;
- de maatregelen van organisatorische aard om verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking van deze gegevens te voorkomen.

In gemeente Haarlem zijn er maatregelen getroffen op deze terreinen. De maatregelen zullen worden opgenomen in het Informatiebeveiligingsplan.

Artikel 15. Slotbepaling

Gegeven de substantiële wijzigingen stellen wij voor om het Reglement gemeentelijke basisadministratie persoonsgegevens van 12 januari 2010 in zijn geheel te vervangen door het onderhavig Reglement basisregistratie personen.

PRIVACYREGLEMENT BRP

Burgemeester en wethouders van de gemeente Haarlem;

gelet op de Wet bescherming persoonsgegevens, de Wet gemeentelijke basisadministratie persoonsgegevens en op de Verordening gemeentelijke basisregistratie personen;

besluiten:

Het privacyreglement voor de gemeentelijke basisregistratie personen van de gemeente Haarlem vast te stellen.

Artikel 1 Begripsbepalingen

Dit reglement verstaat onder:

a.	de wet:	de Wet gemeentelijke basisadministratie persoonsgegevens (Stb. 1994, 494);
b.	besluit:	het Besluit gemeentelijke basisadministratie persoonsgegevens
c.	verordening:	de Verordening gemeentelijke basisadministratie personen vastgesteld door de gemeenteraad d.d. 17 december 2009;
d.	basisadministratie:	de geautomatiseerde verwerking van persoonsgegevens over de bevolking van de gemeente Haarlem als bedoeld in artikel 2 van de wet;
e.	basisregistratie personen:	de basisadministratie aangevuld met de geautomatiseerde verwerking van persoonsgegevens over personen die niet behoren tot de bevolking van de gemeente Haarlem;
f.	GBA-V:	de verstrekkingsvoorziening als bedoeld in artikel 66a van het besluit;
g.	autorisatiebesluit:	een besluit als bedoeld in artikel 91, eerste lid, van de wet betreffende de systematische verstrekking van persoonsgegevens uit de GBA-V of uit de basisadministraties van andere gemeenten;
h.	ingeschrevene:	degene ten aanzien van wie een persoonslijst als bedoeld in artikel 1 van de wet GBA, in de basisadministratie is opgenomen;
i.	geregistreerde:	degene die niet behoort tot de bevolking van de gemeente Haarlem en over wie de verantwoordelijke persoonsgegevens heeft opgenomen in de basisregistratie personen;
j.	authentiek gegeven:	een in de basisregistratie personen opgenomen gegeven dat op grond van artikel 3a van de wet als authentiek wordt aangemerkt;
k.	aangehaakt gegeven:	in de basisregistratie personen over de ingeschrevenen opgenomen gegeven anders dan ter uitvoering van de wet;
l.	verantwoordelijke:	het orgaan dat verantwoordelijk is voor de verwerking van persoonsgegevens in de basisregistratie personen en de uitvoering van het autorisatiebesluit, zijnde het college van burgemeester en wethouders;
m.	bewerker:	degene die, niet werkzaam binnen de gemeentelijke organisatie, het geheel of een gedeelte van het geautomatiseerde systeem onder zich heeft waarmee de basisregistratie personen wordt gevoerd;
n.	beheerder:	de functionaris die namens de verantwoordelijke is belast met de dagelijkse zorg voor de basisregistratie personen en het beheer van het autorisatiebesluit;
o.	afnemer:	bestuursorgaan als bedoeld in artikel 1:1, 1^{e} lid van de Algemene wet bestuursrecht;
p.	binnengemeentelijke afnemer:	elke afnemer die een orgaan is van de gemeente;
q.	derde:	elke andere persoon of instelling dan een afnemer, een ingeschrevene of een geregistreerde;
r.	vrije derde:	een derde als bedoeld in artikel 100 van de wet.

Artikel 2 Beheer van de gemeentelijke basisregistratie personen

1. Beheerder van de gemeentelijke basisregistratie personen is de hoofdafdelingsmanager Dienstverlening.
2. Bewerker van de gemeentelijke basisregistratie personen is hierbij niet van toepassing
3. De beheerder is bevoegd nadere invulling te geven aan:
   a. (te leggen) verbanden met andere gemeentelijke registraties;

b. (rechtstreekse) toegang tot de basisadministratie middels andere geautomatiseerde toepassingen;
c. verstrekkingen aan binnengemeentelijke afnemers of daaraan gelijkgestelden, die geen rechtstreekse toegang hebben tot de basisregistratie personen.

Artikel 3 Authentieke gegevens en verplicht gebruik

1. Met inachtneming van het bepaalde in de artikelen 4, 5 en 6, worden tenminste de authentieke gegevens verstrekt aan alle binnengemeentelijke afnemers die deze gegevens uit de basisregistratie personen nodig hebben voor de vervulling van hun taken, zodanig dat deze afnemers aan hun verplichtingen krachtens de artikelen 3b en 62 van de wet kunnen voldoen.

2. De binnengemeentelijke afnemer die bij de vervulling van zijn taak informatie over een ingeschrevene nodig heeft die in de vorm van een authentiek gegeven beschikbaar is in de basisadministratie, gebruikt voor die informatie dat gegeven.

Artikel 4 Rechtstreekse toegang tot de basisregistratie personen en de GBA-V

1. Rechtstreekse toegang tot de basisregistratie personen hebben:
   a. de beheerder en de door hem aangewezen medewerkers van de afdeling Dienstverlening;
   b. de bewerker en diens medewerkers indien van toepassing, voor zover dat noodzakelijk is voor de uitvoering van de overeenkomst tussen de bewerker en de gemeente;
   c. voor zover niet in een convenant geregeld en voor zover met inachtneming van de artikelen 88 en 89 van de wet de in Bijlage 1 bij dit reglement vermelde binnengemeentelijke afnemers.
2. Voor zover daartoe geautoriseerd krachtens het autorisatiebesluit, hebben de in bijlage 1 genoemde binnengemeentelijke afnemers, rechtstreekse toegang tot de in die bijlage vermelde gegevens in de GBA-V. Zij mogen deze gegevens slechts gebruiken voor de uitvoering van de hun bij wet of door het gemeentebestuur opgedragen taken.
3. Zij hebben de richtlijnen van de beheerder met betrekking tot beveiliging en bescherming van de persoonlijke levenssfeer op te volgen.

Artikel 5 Verstrekking aan binnengemeentelijke afnemers

Met inachtneming van de artikelen 88 en 89 van de wet worden aan de in Bijlage 2 vermelde binnengemeentelijke afnemers de in die tabel aangegeven gegevens systematisch verstrekt ten behoeve van de eveneens in die tabel aangegeven doeleinden.

Artikel 6 Verbanden met andere gemeentelijke registraties

1. Op grond van artikel 96 van de wet, met het oog op het met elkaar in verband brengen, van verwerkingen van persoonsgegevens, worden vanuit de basisregistratie aan de in Bijlage 3 genoemde beheerders van andere gemeentelijke registraties gegevens verstrekt.
2. De betreffende gegevens kunnen in een convenant worden vastgelegd.

Artikel 7 Overige verstrekkingen en de gegevens die kunnen worden verstrekt

Met inachtneming van artikel 100, tweede lid van de wet kunnen, in andere gevallen dan bedoeld in de artikelen 98 en 99 van de wet, aan de in Bijlage 4 bij dit reglement aan te geven overige verzoekers gegevens worden verstrekt voor wat betreft de daarbij aangegeven gegevens en uitsluitend voor de daarbij aangegeven doeleinden en voor zover de persoonlijke levenssfeer daardoor niet onevenredig wordt geschaad.

Artikel 8 Terugmeldplicht

1. Een binnengemeentelijke afnemer die gerede twijfel heeft over de juistheid van een authentiek gegeven dat hij verstrekt heeft gekregen uit de basisregistratie personen, de basisadministratie persoonsgegevens van andere gemeenten of de GBA-V doet hiervan mededeling aan de beheerder.
2. De beheerder regelt de wijze waarop de mededelingen worden gedaan.
3. De beheerder regelt de wijze waarop de kennisgeving aan de binnengemeentelijke afnemer naar aanleiding van een melding wordt gedaan, met inachtneming van het bepaalde in artikel 62 van de wet en de artikelen 62 en 63 van het besluit.
4. In Bijlage 5 worden de binnengemeentelijke afnemers aangewezen die tevens mededeling doen in verband met andere dan authentieke gegevens die aan hen verstrekt zijn. Aangegeven wordt welke gegevens het betreft.

Artikel 9 Protocolplicht

1. Om te kunnen voldoen aan artikel 103 van de Wet en artikel 35 van de Wet bescherming persoonsgegevens, houdt de beheerder van het verstrekken van gegevens een protocol bij.
2. De beheerder voldoet niet aan de verplichting bedoeld in lid 1 voor zover dit verstrekkingen betreft welke noodzakelijk zijn in het belang van de veiligheid van de staat of de voorkoming, opsporing en vervolging van strafbare feiten.

Artikel 10 Recht op inzage en kennisneming van verstrekking

1. Verzoeken om inzage en verzoeken om mededeling van verstrekkingen aan derden ten aanzien van gegevens van geregistreerden en aangehaakte gegevens worden ingediend bij de beheerder.
2. De beheerder beslist namens de verantwoordelijke op de in het eerste lid genoemde verzoeken.
3. De beheerder kan van de verzoeker verlangen dat deze zich in persoon bij hem vervoegt, ter vaststelling van de identiteit van de verzoeker.

Artikel 11 Recht op correctie

1. Verzoeken om verbetering, aanvulling of verwijdering van gegevens van geregistreerden en aangehaakte gegevens worden schriftelijk ingediend bij de beheerder.
2. De beheerder beslist namens de verantwoordelijke op de in het eerste lid genoemde verzoeken.
3. De beheerder kan van de verzoeker verlangen dat deze zich in persoon bij hem vervoegt, ter vaststelling van de identiteit van de verzoeker.

Artikel 12 Verwijdering van gegevens

Gegevens van geregistreerden en aangehaakte gegevens worden door de beheerder uit de basisregistratie personen verwijderd na een daartoe strekkend besluit van de verantwoordelijke. De beheerder verwijdert deze gegevens zo spoedig mogelijk na dit besluit.

Artikel 13 Beveiliging

De beheerder treft ten behoeve van de technische en organisatorische beveiliging de maatregelen als vermeld in het vastgestelde beveiligingsplan.

Artikel 14 Vernietiging

Vernietiging van gegevens van geregistreerden en aangehaakte gegevens geschiedt met inachtneming van de Archiefwet 1995.

Artikel 15 Slotbepaling

1. Dit reglement wordt aangehaald als “Privacyreglement BRP gemeente Haarlem” en treedt in werking op de 1e dag ná die waarop zij bekend is gemaakt;
2. Het privacyreglement GBA van (datum) vervalt ná de inwerkingtreding van dit reglement.
3. Het reglement ligt ter inzage in het gemeentehuis.

Burgemeester en wethouders van de gemeente Haarlem,

De secretaris, De burgemeester,

De heer J. Scholten De heer B. Schneiders

BIJLAGE 1

Lijst van binnengemeentelijke afnemers met een raadpleegmogelijkheid in de basisregistratie en de GBA-V

De medewerkers van de volgende organisatieonderdelen van de gemeente Haarlem hebben rechtstreekse toegang tot de basisregistratie en tot de GBA-V, voor zover daartoe geautoriseerd op grond van het autorisatiebesluit. De bevoegdheid van rechtstreekse raadpleging van de GBA-V, is gebaseerd op het autorisatiebesluit als bedoeld in artikel 1, onder g.

Organisatie onderdeel	Wettelijk kader	Gegevensset
Dienstverlening/Team Balie Dienstverlening/Digiteam Dienstverlening/Flexpool Dienstverlening/PBO (Personen) Dienstverlening/Bedrijfsbureau	Wet GBA, Kieswet, Besluit Burgerlijke Stand, Burgerlijk wetboek, Nationaliteitswetgeving, Wet op de lijkbezorging, Wet justitiële documentatie, Vreemdelingenwet, Paspoortwet en regelgeving rijbewijzen. Wet Inburgering Nieuwkomers	Alle gegevens uit de GBA
Dienstverlening/PBO (Bedrijven en Omgeving)	Huursubsidiewet Huisvestingswet Wet op de huurtoeslag	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Dienstverlening/Team WMO Voorzieningen	Wet Voorzieningen Gehandicapten WMO	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Concernstaf/Bestuur & Management Ondersteuning	Wet Justitiële Documentatie, B&W besluit Toekennen van onderscheidingen en huwelijksjubilarissen. Wet 29/09/1815 Instelling van de Orde van de Nederlandse Leeuw Wet 29/9/1815 instelling van de Orde van Oranje-Nassau en het Besluit van 10 mei 1995, nadere regels Orde van de Nederlandse Leeuw.	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Administratie	Wet Werk en Bijstand	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Beleid en Bedrijfsvoering	Wet Werk en Bijstand ROA	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Debiteurenbeheer en Fraudebestrijding	Wet werk en Bijstand Wetboek van Strafrecht/Strafverordening	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Werk en Inkomen A en B	Wet werk en Bijstand	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Schuldhulpverlening en Budgetbeheer	Wet werk en Bijstand	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Doc. Informatievoorziening	Wet GBA art 96	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Juridische Zaken/Rechtsbesch, Schade en Verz& Invordering, Bezwaar en Beroep	WWB, Cras	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)

Organisatie onderdeel	Wettelijk kader	Gegevensset
Middelen en Services/Controle en Relatiebeheer/GEO Informatie/Basisregistratie	BAG, BIBOP	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Services Financiën/Beheer & Ontwikkeling Fin. Systeem	Wabb	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Politie Kennemerland	HKD, Wet GBA, Politiewet, WPG	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadsbedrijven/Parkeerbeheer	APV	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Jeugd, Onderwijs en Sport/Bureau CARel	Leerplichtwet Leerplichtregeling 1995	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Jeugd, Onderwijs en Sport/ Bureau Leerplicht	Leerplichtwet Leerplichtregeling 1995	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Vastgoed/Vastgoedbeheer	Burgerlijk Wetboek	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Bedrijfsbureau	Woningwet, Awb	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Bedrijfsbureau	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder.	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Bedrijfsbureau/Onderst. Management	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Bedrijfsbureau/Uitvoering afdeling	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)

Organisatie onderdeel	Wettelijk kader	Gegevensset
Veiligheid, Vergunningen en Handhaving/ Handhaving Bebouwde Omgeving/Bureau Procesbegeleiding	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/ Handhaving Bebouwde Omgeving/Bureau Zuid	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Handhaving Openbare Omgeving/Bureau Specifieke Taken	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Omgevingsvergunning/Vergunning verlening	Woningwet, Huisvestingswet, Monumentenwet, APV, Wet ruimtelijke ontwikkeling, Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Wijkzaken/Dagelijks Beheer	Wet economische delicten, Awb, Apv	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Wijkzaken/Dagelijks Beheer en Techniek	Wet economische delicten, Awb, Apv	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
ICT	Het waarborgen van een juiste werking van de computer, het netwerk en de applicaties	Toegang tot alle in het systeem aanwezige gegevens.
Woonservice Kennemerland	Huisvestingswet, Woningwet en convenant	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 4, 10, 11, 12, 13, 14 en 15)
Woningcorporaties Elan Wonen, Pré Wonen en Ymere	Convenant	Maximaal de gegevens zoals overeengekomen in het convenant
GGD Kennemerland	Collegebesluit uitvoering project PHU	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 11, 12, 13, 14 en 15)
RIEC-NH	Regionaal convenant	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)

NB: De invulling van de kolom gegevensset GBA-V blijkt uit de bijlagen bij het voor de gemeente specifieke autorisatiebesluit van de minister van BZK en kan per gemeente verschillen!

De verantwoordelijke (= het College van B&W) kan, indien noodzakelijk nadere aanwijzingen geven met betrekking tot beveiliging en ter bescherming van de persoonlijke levenssfeer.
Alle binnengemeentelijke afnemers beschikken hooguit over een beperkte gedeeltelijke inzage.

BIJLAGE 2

Lijst van binnengemeentelijke afnemers waar systematisch gegevens aan worden verstrekt uit de basisregistratie personen

Organisatie onderdeel	Wettelijk kader	Gegevensset
Middelen en Services/Documentaire Informatievoorziening	Wet GBA, art. 96	Algemene en verwijsgegevens
Stadszaken/Jeugd, Onderwijs en Sport/Leerplicht	Wet GBA, art. 96	Algemene en verwijsgegevens
Sociale Zaken en Werkgelegenheid	Wet GBA, art. 96	Algemene en verwijsgegevens
Stadszaken/Wonen, Welzijn, Gezondheid en Zorg	Wet GBA, art. 96	Algemene gegevens, uitgezonderd persoonsgegevens met indicatie geheimhouding
Regiopolitie Kennemerland	Wet GBA, art. 96	Algemene gegevens van overledenen
Veiligheid, Vergunningen en Handhaving	Wet GBA, art. 96	Algemene en verwijsgegevens

BIJLAGE 3

Lijst van binnengemeentelijke afnemers waaraan, met het oog op het met elkaar in verband brengen van verwerkingen van persoonsgegevens, gegevens worden verstrekt

Organisatie onderdeel	Waarvoor	Gegevensset
Sociale Zaken en Werkgelegenheid	Basisregistratiesysteem DDS/applicatie GWS4all	Alle mutatiegegevens
Stadszaken/Jeugd, Onderwijs en Sport/Leerplicht	CAREL (Centrale administratie RMC en Leerplicht)	Alle mutatiegegevens
Middelen en Services/Documentaire Informatievoorziening	VERSEON	Alle mutatiegegevens

BIJLAGE 4

Lijst van vrije derden waaraan gegevens worden verstrekt

Wie	Waarvoor	Welke categorie	Welke gegevens	Geheimhouding	Leges	Basis
Bibliotheek (geen onderdeel van de gemeente)	Voor de bijhouding van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Buitenlandse EU-overheden	Ter uitvoering van de opgedragen taken en er moet sprake zijn van een Nederlands publiek belang! Advies: toestemming burger vragen.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Buitenlandse niet EU-overheden (met passend beschermingsniveau Art. 76 WBP) www.cbpweb.nl	Ter uitvoering van de opgedragen taken en er moet sprake zijn van een Nederlands publiek belang! Advies: toestemming burger vragen.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA Art. 76 WBP
Buitenlandse rechtspersonen (Voorbeeld: instellingen voor sociale zorg en zekerheid)	Er moet sprake zijn van een Nederlands publiek belang! Vraag de burger om toestemming (zie toelichting).	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA (beperkte verstrek-kings-mogelijk-heden – zie 'Waar-voor')
Caribische landen (Aruba, Curaçao en Sint Maarten) en het Caribisch deel van Nederland (Bonaire, Sint Eustatius en Saba)	Er moet sprake zijn van een Nederlands publiek belang! Vraag de burger om toestemming (zie toelichting).	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA (beperkte verstrek-kings-mogelijk-heden – zie 'Waar-voor')
Crematoria, begraafplaatsen (niet-gemeentelijke)	Voor de bijhouding van registraties verband houdende met het begraven en cremeren.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Culturele organisaties	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Fondsverwervende organisaties	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Instellingen/organisaties ten behoeve van: -Maatschappelijke dienstverlening -Algemene/geestelijke gezondheidszorg	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA

Wie	Waarvoor	Welke categorie	Welke gegevens	Geheimhouding	Leges	Basis
-Kinderopvang -Jeugdwelzijnswerk -Ouderenzorg -Gehandicaptenzorg -Werkvoorziening						
Kerken (niet zijnde de SILA)	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Kredietbank (privaatrechtelijk, bijvoorbeeld een stichting)	Voor de aan deze organisatie opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Inburgeringsbureaus (niet gemeentelijk)	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Migrantenorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Natuurlijke personen	Vooraf schriftelijke toestemming betrokkene (persoon/gezaghouder)	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Onderwijsinstellingen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Ouderenorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Patiëntenverenigingen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Pensioenfondsen	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Plaatselijke afdelingen van politieke partijen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Reclassering/verslaafden-zorg	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Sportorganisaties en -verenigingen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Thuiszorgorganisaties	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Vakorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Verenigingen en stichtingen met maatschappelijk of filantropisch doel	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Vrouwenorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Woningbouwverenigingen/woningcorporaties	Ten behoeve van de bijhouding van de huurdersadministratie en de woningtoewijzing	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Ziekenhuizen	Voor het uitoefenen van patiëntenzorg, het verlenen van medische zorg en het innen van rekeningen ivm die zorg	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA

Toelichting 'vrije derde'

Scholen

Scholen hebben persoonsgegevens nodig voor een juiste registratie in de leerlingenadministratie. Vaak wordt de leerling gevraagd om een afschrift uit de GBA in te leveren. Een afschrift uit de GBA is echter vaak helemaal niet nodig. Zie hiervoor het artikel 'GBA-uittreksel niet nodig bij inschrijving school' in Burgerzaken & Recht, jaargang 2001, nummer 6, pagina 186-187.
De commissie meent dat er geen grond is om op basis van de Wet GBA gegevens te **moeten** verstrekken aan scholen. Aan de burger zelf kan echter altijd een uittreksel van zichzelf of zijn minderjarig kind worden verstrekt als hij dit toch wenst. Geef wel de informatie dat
het voor dit doel niet nodig is. Er worden aan de burger wel leges in rekening gebracht als hij toch een uittreksel wenst voor dit doel.

Caribische landen en het Caribische deel van Nederland

De Caribische landen zijn: Aruba, Curaçao en Sint-Maarten.
Onder het Caribisch deel van Nederland vallen: Bonaire, Sint-Eustatius en Saba (openbare lichamen BES). De Wet GBA is geen rijkswet en daarom alleen van toepassing op het Europees deel van Nederland. De Wet Basisadministraties persoonsgegevens BES is alleen van toepassing op het Caribische deel van Nederland (openbare lichamen BES).
Aruba, Curaçao en Sint-Maarten zijn zelfstandige Caribische landen binnen het Nederlandse Koninkrijk en hebben hun eigen verordeningen.

Ten aanzien van deze landen en gebiedsdelen is het mogelijk om gegevens uit de GBA te verstrekken op grond van:

1. artikel 100a van de Wet GBA
   De gegevensuitwisseling op grond van dit artikel vindt slechts plaats in het kader van de bijhouding van de GBA en de bevolkingsadministraties van de Caribische landen en het Caribische deel van Nederland.

2. artikel 100 van de Wet GBA
   De Caribische landen en het Caribisch deel van Nederland zijn aan te merken als (vrije) derden in de zin van de Wet GBA. Dit maakt verstrekking op grond van artikel 100 Wet GBA mogelijk.

Verstrekking aan buitenlandse overheidsinstellingen of buitenlandse rechtspersonen

De GBA is er voor de Nederlandse overheid. Verstrekkingen aan andere verzoekers (derden) worden zo nodig expliciet mogelijk gemaakt door de Wet GBA.
De verstrekking aan buitenlandse overheidsorganen (ongeacht of dit nationale, regionale of gemeentelijke overheden in het land zelf zijn dan wel ambassades en consulaten van die landen in Nederland) of buitenlandse rechtspersonen is niet expliciet geregeld in de Wet GBA. Dit betekent dat verstrekking van gegevens uit de GBA aan buitenlandse overheidsinstellingen of buitenlandse rechtspersonen alleen aan de orde is op grond van artikel 98 (verstrekking van gegevens is voorgeschreven in Nederlands algemeen verbindend voorschrift – zie bij 'Verplichte derde') en 100 (volgens de gemeentelijke verordening en aan rechtspersonen zonder winstoogmerk of natuurlijke personen) Wet GBA.

De verstrekking op grond van artikel 100 Wet GBA moet gerechtvaardigd worden door een 'dringende maatschappelijke behoefte', zoals benoemd in de Wet GBA, artikel 100, lid 1 onder a. Dit betekent dat er sprake moet zijn van een Nederlands publiek belang. Dat kan liggen in het feit dat de buitenlandse verzoeker de gegevens nodig heeft voor de uitvoering van een Nederlands algemeen verbindend voorschrift dan wel voor een doel dat, met het oog op een publiek belang, expliciet in de gemeentelijke verordening is voorgeschreven.
In het laatste geval kan bijvoorbeeld worden gedacht aan verstrekking van gegevens aan private, niet commerciële instellingen op het terrein van zorg (bijvoorbeeld: ziekenhuizen) of maatschappelijk welzijn in buitenlandse grensgemeenten, waar ook de eigen inwoners gebruik van maken, zodat de wachtlijsten in de Nederlandse instellingen kunnen worden weggewerkt.

Bij een verstrekking op grond van artikel 100, sub a, Wet GBA gelden altijd de eisen van proportionaliteit en subsidiariteit. Dat houdt in dat de verstrekking in een juiste verhouding moet staan tot het nagestreefde doel en dat het doel niet op een minder ingrijpende wijze kan worden bereikt.

Naar aanleiding van antwoorden op kamervragen die de afgelopen jaren aan bewindspersonen over dit onderwerp zijn gesteld, adviseert de NVVB uit voorzorg om de burger vooraf uitdrukkelijk toestemming te laten verlenen voor dergelijke verstrekkingen.

Als een verzoek niet voldoet aan de kaders die artikel 98 of 100 van de Wet GBA stelt, moet een verzoek van een buitenlandse instelling (waaronder de ambassade of het consulaat van dat land) worden afgewezen.

(Zie voor verstrekkingen aan buitenlandse advocaten de toelichting bij ‘Schema 3 Verplichte derden’)

Extra toetsingscriterium bij verzoek van buiten de EU

EU
De meeste verzoeken waar de voorgaande paragraaf op doelt zullen afkomstig zijn vanuit een ander land **binnen** de Europese Unie.
Niet EU
Artikel 100, lid 3, van de wet GBA noemt een extra toetsingspunt bij verzoeken van **buiten** de Europese Unie. In de Wet Bescherming Persoonsgegevens staan specifieke bepalingen voor gegevensverkeer naar deze landen. De hoofdregel is dat persoonsgegevens alleen mogen worden doorgegeven aan landen met een passend beschermingsniveau. Een overzicht van landen die een passend beschermingsniveau hebben kunt u vinden op www.cbpweb.nl als
u zoekt met de zoekterm 'passend beschermingsniveau'.

Hoe moet u omgaan met een verzoek van een buitenlandse overheidsinstantie of rechtspersoon?

De gevraagde gegevens zullen soms al, buiten de GBA om, op grond van een andere internationale regeling kunnen worden verstrekt en in dat geval is verstrekking uit de GBA niet aan de orde. Op basis van afspraken op internationaal niveau vindt er namelijk ook uitwisseling plaats van persoonsgegevens op specifieke terreinen. Denk hierbij niet alleen aan uitwisseling van gegevens op het gebied van de burgerlijke stand in het kader van de CIEC, maar bijvoorbeeld ook aan verstrekking van gegevens in verband met alimentatieverplichtingen of aan verkeersovertredingen die in het buitenland begaan worden door Nederlandse ingezetenen.
In een aantal gevallen is het verzoek dat de ambtenaar van de GBA ontvangt dan ook gericht aan het verkeerde ‘loket’. De ambtenaar kan dan doorverwijzen of het verzoek doorsturen naar een andere overheidsinstelling, oftewel een ander ‘loket’. Denk hierbij aan de verzoeken die gericht moeten worden aan de Internationale Rechtshulp Centra (IRC). Ook verzoeken inzake internationale alimentatieverplichtingen moeten niet bij de gemeente, maar bij het Landelijk Bureau Inning Onderhoudsbijdragen (LBIO) worden ingediend.

Het komt geregeld voor dat er in een verzoek van een ambassade of een consulaat verwezen wordt naar het Verdrag van Wenen inzake consulair verkeer van 24 april 1963. Daarin staat dat vertegenwoordigingen van andere landen toegang moeten kunnen krijgen tot hun onderdanen.
Dit verdrag regelt echter niet de ‘toegang’ tot de GBA. Artikel 36 van het verdrag geeft het recht aan een consulaire ambtenaar om een onderdaan te bezoeken, die bijvoorbeeld in een gevangenis of ziekenhuis verblijft. In dat geval vraagt de politie, respectievelijk het ziekenhuispersoneel, aan betrokkene of hij of zij dat goed vindt. Er wordt dus expliciet toestemming gevraagd aan betrokkene. Het verdrag regelt dus alleen de toegang tot de persoon zelf en niet tot zijn persoonsgegevens. De gemeente moet het schriftelijke verzoek om informatie dus afwijzen om bovenstaande redenen.

BIJLAGE 5

Lijst van binnengemeentelijke afnemers, die zijn aangewezen tevens mededeling te doen in verband met andere dan authentieke gegevens die aan hen verstrekt zijn.

Organisatieonderdeel	Gegevens