

advies  
aan b&w

Sector	: Inwoners	Openbaar: <input checked="" type="checkbox"/>
Afdeling	: Management ondersteuning Inwoners	Niet openbaar: <input type="checkbox"/>
Zaaknummer(s) Ingekomen stuk(ken)	:	Kabinet: <input type="checkbox"/>
Behandelend medewerk(st)er	: M. Aerds Tel.: (0495) 575 416	
Portefeuillehouder(s)	: A.A.M.M. Heijmans	Nummer B&W-advies: BW-004226

**ONDERWERP**

Informatie beveiliging Burgerzaken

**ADVIES**

Instemmen met bijgevoegde rapportage met betrekking tot de informatiebeveiliging Burgerzaken

**TOELICHTING**

[Invulinstructie]

Relatie met vorig voorstel:  
Informatie beveiliging Burgerzaken 2010.

Algemeen:

In de wettelijke voorschriften met betrekking tot de Gemeentelijke basisadministratie persoonsgegevens (GBA) zijn bepalingen opgenomen over de beveiliging van de GBA. Gemeenten zijn verplicht zorg te dragen voor de nodige voorzieningen van technische en organisatorische aard. Deze voorzieningen omvatten ten minste maatregelen gericht op:

- personen;
- de toegang tot gebouwen en ruimten;
- een deugdelijke werking en beveiliging van apparatuur en programmatuur;
- het beheer van gegevens;
- geheimhouding van de in de basisadministratie vermelde gegevens;
- calamiteiten.

Gemeenten moeten één keer per 3 jaar een GBA audit laten uitvoeren. De huidige GBA audit bestaat uit drie delen, waaronder het procesdeel. Het procesdeel bevat de toets van processen rondom de opslag en beveiliging van gegevens. In de vragenlijst van het procesdeel zijn vragen opgenomen die betrekking hebben op controle en rapportage.

Weert, 7 december 2011  De directeur,	S	B	W	W	W	W
	akkoord					
	bespreken					
Behandeling uiterlijk in college van 3 januari 2012						
<b>Akkkoord met advies</b>						

Beslissing d.d.:

Nummer: 12

De secretaris

03 JAN. 2012

Totaal aantal pagina's 3

Eenmaal per jaar dient aan uw College een managementrapportage te worden uitgebracht waarin wordt aangegeven in welke mate de gewenste garanties en waarborgen ten aanzien van de betrouwbaarheidseisen van de GBA worden bereikt. Deze betrouwbaarheidseisen houden de volgende punten in:

- de beschikbaarheid van het GBA informatiesysteem;
- de vertrouwelijkheid van de GBA gegevens;
- de integriteit van de GBA gegevens;
- de controleerbaarheid van de GBA gegevens.

Deze toets houdt tevens een evaluatie in van de uitvoering van de vereiste maatregelen.

**Argumenten:**

De interne audit van de GBA die in 2011 is uitgevoerd heeft zich vooral gericht op de verdere invoering van de in 2010 en voorgaande jaren voorgestelde maatregelen.

In 2011 zijn diverse toetsingen uitgevoerd. De constatering zijn conform de bepalingen in de wetgeving aan het management van de sector gerapporteerd.

Bij de toetsingen wordt elk jaar aan een ander onderwerp extra aandacht besteed en in 2011 is vooral stil gestaan bij de autorisatie van de toegang tot de GBA gegevens van gebruikers van overige applicaties.

Door het leggen van koppelingen tussen diverse geautomatiseerde systemen en de invoering van de Basisadministratie Personen (BAP) is het noodzakelijk dat het correct verlenen van autorisaties en het gebruik van gegevens ook wordt toegepast binnen andere informatiesystemen, bijvoorbeeld het centrale gegevensmagazijn (makelaar).

De toepassing van de autorisatietabellen die aan het gebruik van persoonsgegevens vanuit de GBA gekoppeld zijn, zal in de toekomst vanuit de BAP georganiseerd moeten worden.

De eenheid Burgerzaken zal als applicatiebeheerder van de GBA gegevens verantwoordelijk zijn voor de juistheid van de gegevens.

De autorisatie van de toegang tot de persoonsgegevens zal nadrukkelijk aandacht moeten krijgen in de verdere structurering van het BAP.

Voor de actuele stand van zaken met betrekking tot de aanbevelingen wordt korthedshalve verwezen naar bijgevoegd overzicht.

De algemene conclusie van de uitgevoerde Interne Controle is op dit moment dat de meeste aanbevelingen te maken hebben met een verdere optimalisering van beleidsdocumenten, bijv. een gemeentebreed beleidsdocument informatiebeveiliging en een gemeentebreed noodplan fysieke uitwijk. Het zwaartepunt van de aanbevelingen heeft te maken met onderwerpen waarbij de eenheid Burgerzaken afhankelijk is van ontwikkelingen in andere organisatieonderdelen of zelfs landelijke ontwikkelingen.

Voor de dagelijks voorkomende werkzaamheden zijn de nodige maatregelen getroffen, zodat de eenheid Burgerzaken kan voldoen aan de zorgvuldigheid die geëist wordt bij de omgang met persoonsgegevens.

**Kanttekeningen:**

Niet van toepassing.

**JURIDISCHE GEVOLGEN (o.a. FATALE TERMIJNEN/HANDHAVING)**

Niet van toepassing.

## **FINANCIËLE EN PERSONELE GEVOLGEN**

Niet van toepassing.

## **COMMUNICATIE/PARTICIPATIE**

Voor wie is dit advies van belang?:

❖ Interne organisatie

*Nadere specificatie:* Eenheid Burgerzaken

Geadviseerd wordt de volgende communicatie-instrumenten te gebruiken:

❖ Niet van toepassing

Geadviseerd wordt de volgende participatie-instrumenten te gebruiken:

❖ Niet van toepassing

## **OVERLEG GEVOERD MET**

Intern:

Eenheid Burgerzaken, afdeling Informatievoorziening.

Extern:

nvt

## **BIJLAGEN**

Openbaar:

Overzicht aanbevelingen en aandachtspunten controle - en analysewerkzaamheden GBA 2011

Niet-openbaar:

Niet van toepassing

## Overzicht aanbevelingen en aandachtspunten controle – en analysewerkzaamheden GBA 2011 ( uitgevoerd november 2011 )

Onderwerp	Verantwoordelijkheid	Bevindingen Interne Controle 2010.	Constatering of aanbeveling op basis van uitgevoerde Interne Controle 2011.
In het kader van het Informatiebeveiligingsbeleid dient er een controlemogelijkheid op beschikbaarheid van het GBA informatiesysteem aanwezig te zijn. De toegankelijkheid van gegevens in het GBA informatiesysteem moet op jaarbasis gemiddeld 96% zijn. Er dient een risicoanalyse uitgevoerd te zijn.	I&A in samenwerking met Burgerzaken	Het meetinstrument Nagios laat de "uptime" van de AS400 zien. Er worden nog afspraken gemaakt over het periodiek verstrekken van overzichten m.b.t. de beschikbaarheid van de AS400 en hiermee het GBA informatiesysteem.	De Afdeling I&A verstrekt aan de eenheid Burgerzaken een overzicht van de beschikbaarheid van het systeem over het afgelopen jaar. De eenheid Burgerzaken heeft I&A verzocht dit overzicht vanaf 2012 maandelijks te verstrekken.
	Burgerzaken	De risicoanalyse is in november 2010 geactualiseerd en vastgesteld. De borging van de jaarlijkse analyse in de werkprocessen dient nog doorgevoerd te worden.	Het uitvoeren van een risicoanalyse, dreigingsanalyse en maatregelenanalyse (informatiebeveiligingsplan) zou bij uitstak thuishoren bij een controller die niet betrokken is bij de uitvoering van procedures en werkzaamheden binnen Burgerzaken.
De gemeente moet beschikken over een actueel en vastgesteld (informatie)beveiligingsplan	Burgerzaken	Het nieuwe ( informatie ) beveiligingsplan is in november 2010 geactualiseerd en door het college vastgesteld.	Onderzocht wordt of ondersteuning kan worden ingekocht. Adviesbureau BMC biedt bijv. de gemeenten het Informatiebeveiligingsplan GBA en waardedocumenten aan.
Jaarlijkse instructie aan medewerkers over mogelijke risico's en (verplichtende) richtlijnen en procedures om schade en incidenten te voorkomen.	Burgerzaken	Het verslag van het werkoverleg is in het dossier t.b.v. de audit opgenomen.	Het onderwerp "Risicobewustzijn" wordt in het afdelingsoverleg van 6 december a.s. besproken.
Medewerkers dienen jaarlijks te bevestigen dat zij kennis hebben genomen van voorschriften en procedures.	Burgerzaken	Door middel van een e-mailbericht worden alle medewerkers herinnerd dat de bevestiging herhaald dient te worden.	Aankondiging in het afdelingsoverleg. Een herinnering wordt eventueel verzonden d.m.v. een e-mail.

Onderwerp	Verantwoordelijkheid	Interne Controle2010.	Constatering of aanbeveling op basis van uitgevoerde Interne Controle2011.
De gemeente dient te beschikken over een actuele procedure voor het verwerken van terugmeldingen van binnen- en buitengemeentelijke afnemers.	Burgerzaken	Nog niet opgesteld. Heeft relatie met Decos en BAG : discussie gaande over vormgeving.	Opstelling dient nog plaats te vinden.
De gemeente moet beschikken over een actuele procedure voor het verwerken van incidentmeldingen.	Burgerzaken	Geadviseerd werd om voor de bepaling van de actualiteit in het document een versie aanduiding en datum vaststelling op te nemen. Het versiebeheer is gedeeltelijk toegepast.	Versiebeheer is aangevuld.
De termijnen waarbinnen de incidentmelding moet zijn verwerkt moeten zijn vastgelegd.	Burgerzaken	De termijnen zijn in de procedure vastgelegd.	Geen opmerkingen.
De wijze waarop de melder wordt bericht hoe de melding is verwerkt moet vastliggen.	Burgerzaken	Terugkoppeling was niet beschreven. De procedure is hiermee aangevuld.	Geen opmerkingen.
Van de incidentmelding wordt een registratie bijgehouden of verslag opgemaakt.	Burgerzaken	Er werd geen registratie van meldingen bijgehouden. De procedure is hiermee aangevuld.	Geconstateerde incidenten met betrekking tot inloggen (autorisaties) wordt door de applicatiebeheerder GBA geregistreerd.
De gemeente dient te beschikken over een actueel draaiboek (noodplan) waarin alle taken, verantwoordelijkheden en acties zijn vastgelegd in geval dat de hoofdlocatie niet meer gebruikt kan worden.	Burgerzaken	Globaal noodplan aanwezig. Geadviseerd werd dit te actualiseren en datum vaststelling te vermelden. Aanpassing van het noodplan was op moment van interne controle nog in uitvoering.	De samenhang in applicaties en de onderliggende systemen worden momenteel in kaart gebracht door de applicatiebeheerders. Op basis van deze samenhang wordt ook een vervolg gegeven aan de organisatie van de noodzakelijke uitwijkvoorzieningen.

Onderwerp	Verantwoordelijkheid	Interne Controle2010.	Constatering of aanbeveling op basis van uitgevoerde Interne Controle2011.
<p>Het draaiboek is altijd beschikbaar, ook indien de reguliere locatie niet beschikbaar is.</p> <p>Na de vereiste back-up van gegevens naar het back-up medium dient een handmatige of geautomatiseerde toets plaats te vinden of de gegevens zijn geverifieerd en kunnen worden teruggelezen.</p>	<p>Burgerzaken</p> <p>Burgerzaken / I en A</p>	<p>Document aanwezig op back-up van systemen maar er kon niet worden vastgesteld of document op dislocatie aanwezig was.</p> <p>Nu niet standaard. Alleen op verzoek van de afdeling Burgerzaken wordt een dergelijke controle uitgevoerd.</p> <p>Verder onderzoek naar geautomatiseerd controleproces heeft uitgewezen dat dit in verband met de te lange doorlooptijd van dit proces niet mogelijk is.</p>	<p>Geadviseerd wordt het draaiboek op de dislocatie op papier beschikbaar te hebben.</p> <p>Dagelijks wordt de back up tape gewisseld door ICT services. Deze tape gaat naar de kluis ( externe locatie ). Als de tape "uitgeworpen" is, is de back-up goed gegaan. In de gevallen dat er iets niet goed is gegaan, blijft de tape zitten. Pas op dat moment wordt er actie ondernomen in die zin dat dit gemeld wordt bij BZ. BZ bewaard mutatieverslagen dan langer en de ingenomen reisdocumenten worden later vernietigd.</p>

Naast bovenstaande aandachtspunten zijn de overige te toetsen elementen op basis van de wet- en regelgeving in de interne controle bekeken. De uitgevoerde interne controle gaf verder geen reden tot het maken van een opmerking.