

advies
aan b&w

Sector	: Inwohers	Openbaar: <input checked="" type="checkbox"/>
Afdeling	: Publiekszaken	Niet openbaar: <input type="checkbox"/>
Zaaknummer(s) ingekomen stuk(ken)	:	Kabinet: <input type="checkbox"/>
Behandelend medewerk(st)er	: Mia Aerds Tel.: (0495) 575 416	
Portefeuillehouder(s)	: A.A.M.M. Heijmans	Nummer B&W-advies: BW-005782

ONDERWERP

Informatiebeveiliging Publiekszaken.

ADVIES

Instemmen met bijgevoegde rapportage met betrekking tot de informatiebeveiliging Publiekszaken.

TOELICHTING

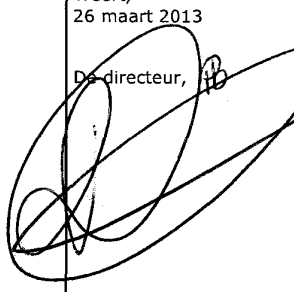

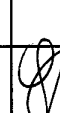

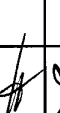
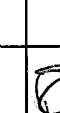

Relatie met vorig voorstel:
Informatiebeveiliging Burgerzaken 2011.

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 tenminste 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, 26 maart 2013 De directeur, 		S		B	W	W	W	W
		akkoord						
		bespreken						
Behandeling uiterlijk in college van 2 april 2013								

Beslissing d.d.:

AKKOORD met advies**02 APR. 2013**Nummer: **2**De secretaris, Totaal aantal pagina's: 3
Pagina 1

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 2012 is uitgevoerd heeft zich vooral gericht op de verdere invoering van de in 2011 en voorgaande jaren voorgestelde maatregelen.

In 2012 zijn diverse toetsingen uitgevoerd. De constatering is 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. In 2012 is vooral stil gestaan bij de autorisatie van de toegang tot de GBA gegevens van gebruikers van overige applicaties. Vooral zullen er in maatregelen getroffen moeten worden om de toegang tot de persoonsgegevens door medewerkers van het KCC te stroomlijnen op een manier waar zowel de dienstverlening richting de burgers als de wettelijke bepalingen in het kader van de bescherming van de persoonsgegevens recht gedaan kunnen worden.

Door het leggen van koppelingen tussen diverse geautomatiseerde systemen is het noodzakelijk dat het correct verlenen van autorisaties en het gebruik van gegevens ook wordt toegepast binnen andere informatiesystemen, zoals het KCS dat bij het KCC in gebruik is.

De toepassing van de autorisatietabellen die aan het gebruik van persoonsgegevens vanuit de GBA gekoppeld zijn moet hierbij uitgangspunt zijn.

De informatiebeheerder en de gegevensbeheerder van de GBA zijn als eerste aanspreekpunt verantwoordelijk voor de juistheid van de gegevens.

De autorisatie van de toegang tot de persoonsgegevens zal nadrukkelijk aandacht moeten krijgen in de verdere structurering van de koppeling tussen de diverse systemen.

Voor de actuele stand van zaken met betrekking tot de aanbevelingen wordt kortheidshalve 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 afdeling Publiekszaken afhankelijk is van ontwikkelingen in andere organisatieonderdelen of zelfs landelijke ontwikkelingen.

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

Kanttekeningen:

De huidige GBA-audit wordt vervangen door een jaarlijkse zelfevaluatie met behulp van een evaluatie-instrument. De inwerkingtreding is afhankelijk van wijziging van wetgeving.

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:* Afdeling Publiekszaken

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:

Afdeling Publiekszaken.

Extern:

nvt

BIJLAGEN

Openbaar:

Overzicht aanbevelingen en aandachtspunten controle – en analysewerkzaamheden GBA 2012.

Niet-openbaar:

Niet van toepassing

Overzicht aanbevelingen en aandachtspunten controle - en analysewerkzaamheden GBA 2012 (uitgevoerd november 2012)

Onderwerp	Verantwoordelijkheid	Bevindingen Interne Controle 2011.	Constatering of aanbeveling op basis van uitgevoerde Interne Controle 2012.
<p>In het kader van het Informatiebeveiligingsbeleid dient er een controlemogelijkheid op beschikbaarheid van het GBA informatiesysteem aanwezig te zijn.</p> <p>De toegankelijkheid van gegevens in het GBA informatiesysteem moet op jaarbasis gemiddeld 96% zijn.</p> <p>Er dient een risicoanalyse uitgevoerd te zijn.</p>	<p>PIF in samenwerking met Publiekszaken</p>	<p>De Afdeling PIF verstrekt aan de afdeling Publiekszaken een overzicht van de beschikbaarheid van het systeem AS400 en hiermee het GBA informatiesysteem over het afgelopen jaar.</p> <p>De afdeling Publiekszaken heeft PIF verzocht dit overzicht vanaf 2012 maandelijks te verstrekken.</p>	<p>Dat overzicht wordt maandelijks gemaaid naar i.bijnen@weert.nl.</p> <p>De uptime valt binnen de normen. Uptime AS400 is echter niet het zelfde als beschikbaarheid GBA. Deze kan niet worden gemeten.</p>
	<p>Publiekszaken</p>	<p>De risicoanalyse is in november 2010 geactualiseerd en vastgesteld.</p> <p>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 uitstek thuishoren bij een controller die niet betrokken is bij de uitvoering van procedures en werkzaamheden binnen Publiekszaken.</p>	<p>Voor het onderwerp informatiebeveiliging is voor 2013 een prioriteit ingediend, die is ingewilligd. Hierdoor wordt in 2013 een risico-analyse uitgevoerd.</p>
<p>De gemeente moet beschikken over een actueel en vastgesteld (informatie)beveiligingsplan</p>	<p>Publiekszaken</p>	<p>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 Informatie-beveiligingsplan GBA en waardedocumenten aan.</p>	<p>Voor het onderwerp informatiebeveiliging is voor 2013 een prioriteit ingediend, die is ingewilligd. Hierdoor wordt in 2013 opdracht verstrekt aan een adviesbureau om het informatiebeveiligingsplan vorm te geven.</p>
<p>Jaarlijkse instructie aan medewerkers over mogelijke risico's en (verplichtende) richtlijnen en procedures om schade en incidenten te voorkomen.</p>	<p>Publiekszaken</p>	<p>Het onderwerp "Risicobewustzijn" wordt in het afdelingsoverleg van 6 december 2011 besproken.</p>	<p>Het onderwerp "Risicobewustzijn" wordt in het afdelingsoverleg Publiekszaken van december 2012 besproken.</p>

Medewerkers dienen jaarlijks te bevestigen dat zij kennis hebben genomen van voorschriften en procedures.	Publiekszaken	Aankondiging dat de bevestiging herhaald moet worden in het afdelingsoverleg. Een herinnering wordt eventueel verzonden d.m.v. een e-mail.	Dit wordt besproken in het afdelingsoverleg Publiekszaken in december 2012.
Onderwerp	Verantwoordelijkheid	Interne Controle 2011.	Constatering of aanbeveling op basis van uitgevoerde Interne Controle 2012.
De gemeente dient te beschikken over een actuele procedure voor het verwerken van terugmeldingen van binnen- en buitengemeentelijke afnemers.	Publiekszaken	Nog niet opgesteld. Heeft relatie met Decos en BAG : discussie gaande over vormgeving.	Deze is te vinden op intranet. http://srv-cms/Smartsite.shtml?ch=Tra&id=59389
De gemeente moet beschikken over een actuele procedure voor het verwerken van incidentmeldingen.	Publiekszaken	Voor de bepaling van de actualiteit in het document wordt een versie aanduiding en datum vaststelling opgenomen.	Akkoord.
De termijnen waarbinnen de incidentmelding moet zijn verwerkt moeten zijn vastgelegd.	Publiekszaken	De termijnen zijn in de procedure vastgelegd.	Akkoord.
De wijze waarop de melder wordt bericht hoe de melding is verwerkt moet vastliggen.	Publiekszaken	De procedure is hiermee aangevuld.	Akkoord.
Van de incidentmelding wordt een registratie bijgehouden of verslag opgemaakt.	Publiekszaken	Geconstateerde incidenten met betrekking tot inloggen (autorisaties) wordt door de applicatiebeheerder GBA geregistreerd.	Deze worden geregistreerd bij geconstateerde afwijking. 2012 niet van toepassing.
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.	Publiekszaken	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.	Hiervoor komen we maandelijks bij elkaar, de noodzaak is duidelijk, er zijn stappen gezet. Het is nu zaak alles eenduidig te gaan vastleggen. Hier is project voor opgestart onder leiding van Harrie van Helvoort.

Onderwerp	Verantwoordelijkheid	Interne Controle 2011.	Constatering of aanbeveling op basis van uitgevoerde Interne Controle 2012.
Het draaiboek is altijd beschikbaar, ook indien de reguliere locatie niet beschikbaar is.	Publiekszaken	Document aanwezig op back-up van systemen maar er kon niet worden vastgesteld of document op dislocatie aanwezig was. Geadviseerd wordt het draaiboek op de dislocatie op papier beschikbaar te hebben.	Dit past niet in het beleid papierloos te gaan werken. Er zal in 2013 naar gekeken worden hoe en waar de informatie te raadplegen is.
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.	Publiekszaken / PIF	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.	

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.