GBA audit: niet langer een 'papieren' tijger

Het zal u niet zijn ontgaan dat per 1 juli 2002 de Regeling periodieke audits grondig is gewijzigd. Met name de eisen voor het procesdeel zijn ingrijpend gewijzigd en de meetlat is een stuk hoger komen te liggen. In dit artikel wordt ingegaan op deze veranderingen. De GBA audit wordt uitgevoerd sinds de tweede helft van 1999. In deze periode zijn alle gemeenten tenminste éénmaal beoordeeld door een door de Raad voor Accreditatie gecertificeerde audit-instelling. Bestuur en Management Consultants (BMC) is één van de drie GBA audit instellingen[1] .

Drs. M.B.H. IJpelaar CISA
Senior adviseur BMC Leusden.

Audit wordt langzaam zwaarder
Door het Agentschap BPR wordt de audit gepresenteerd als een 'groeimodel'. Dat betekent dat de verplichtingen om te voldoen aan de eisen, langzaam worden opgeschroefd. Wat dit inhoudt hebben gemeenten aan den lijve ondervonden: per 1 januari 2001 is onder druk van de Tweede Kamer het privacydeel aan de GBA-audit toegevoegd. Daarmee bestaat de GBA-audit uit drie onderdelen:

- *Inhoudelijk deel*. Hierbij wordt de integriteit van de GBA-gegevens beoordeeld. Daarbij wordt gekeken naar het administratief correct en betrouwbaar zijn van de persoonsgegevens uitgaande van de kwaliteitsnormen zoals die door BPR zijn neergelegd in de Regeling periodieke GBA-audit.

- *Procesdeel*. Hierbij ligt de focus met name op de beschikbaarheid van de persoonsgegevens. Dit houdt in dat geen gegevens verloren mogen gaan en dat de GBA-gegevens en de GBA-applicatie op ieder gewenst moment beschikbaar zijn. Vanaf 1 juli 2002 is de beveiliging van de GBA een verplicht kwaliteitsaspect.

- *Privacydeel*. Hierbij wordt de vertrouwelijkheid van de GBA deels beoordeeld. Dit houdt in dat informatie geen bredere verspreiding krijgt dan strikt noodzakelijk en wenselijk.

Inmiddels is de eerste volledige auditronde achter de rug: alle gemeenten hebben een GBA-audit ondergaan. Uit de door BPR periodiek gepubliceerde resultaten blijkt dat circa 1/3 van de gemeenten ongeschonden door de audit heen komt en dat 2/3 van de gemeenten 'zakt'. Ongeveer 10% slaagt niet voor de inhoudelijke audit. Met name het proces- en het privacydeel van de audit vormen een bottleneck. Niettemin zijn onder andere naar aanleiding van de door Het Expertise Centrum uitgevoerde evaluatie van het auditinstrument de eisen bij het procesdeel per 1 juli j.l. behoorlijk aangescherpt. De communicatie hierover door BPR is tot dusver summier geweest, zodat verwacht mag worden dat het aandeel van de gemeenten dat ongeschonden door de audit komt, spectaculair zal dalen. Hier zal later in dit artikel op worden teruggekomen.

Wijzigingen in het audit-regime
Door BPR is vastgesteld dat in principe alle na 1 juli 2002 uit te voeren GBA-audits onder het nieuwe juridische regime vallen. Uitzonderingen op deze hoofdregel zijn slechts mogelijk door schriftelijke tussenkomst van BPR.
Verder is het zo dat her-audits in principe altijd onder het juridisch regime plaatsvinden van de voorafgaande GBA-audit. Dat wil bijvoorbeeld zeggen dat wanneer er bij de audit nog geen privacydeel van toepassing was, dit ook niet zal worden beoordeeld bij de her-audit.

[1] *Zie besluit d.d. 30 augustus 1999/Nr. BPR99/80396 (Staatscourant 1999, nr. 170).*

Wat is er veranderd na 1 juli 2002?

- Gemeenten worden niet langer per half jaar maar per kwartaal ingedeeld. Hierdoor wordt de werklast bij de auditinstellingen verspreid over vier piekperioden per jaar in plaats van twee.
- Er wordt een wettelijke termijn gesteld aan de oplevering van auditrapportages. De conceptrapportage moet binnen 2 maanden na de start van de audit worden opgeleverd. Deze rapportage moet worden besproken met de gemeente op basis van het principe 'hoor en wederhoor' en vervolgens na twee maanden definitief worden gemaakt
- De auditinstelling behoort concrete aanbevelingen te doen om de bij het proces- en privacydeel geconstateerde risico's op te heffen of te verlagen. Omdat dit meer werk met zich meebrengt wordt de auditvergoeding verhoogd met € 1.100,--.
- De gemeente krijgt maximaal één werkweek vóór de inhoudelijke audit te horen welke A-nummers zijn geselecteerd voor de steekproef
- De eisen op grond waarvan afwijkingen als structureel kunnen worden bestempeld zijn vastgelegd. De auditinstellingen bleken onderling afwijkende posities in te nemen. Structurele fouten hebben betrekking op: Een schriftelijk aantoonbare procedurefout in de administratieve organisatie en op een schriftelijk aantoonbare fout in de GBA-applicatie. Een afwijking, die als structurele fout is bestempeld bij voorgaande (her-)audits, geldt niet meer. Om deze reden moet de gemeente de (her-)auditrapportages aanleveren.
- De bewaartermijn van (her)auditrapportages is 7 jaar
- Er worden bij de inhoudelijke audit geen brondocumenten meer gevraagd voor categorie 12 Reisdocumenten. Dit betekent een aanzienlijke verlichting van de werklast.

Verzwaring van het procesdeel

Zoals eerder gemeld, wordt het procesdeel veel zwaarder. Dit ligt met name aan de diepgang van de uit te voeren audit. Bij de diepgang wordt, analoog aan de accountancy-praktijk, onderscheid gemaakt in opzet, bestaan en werking. Zo betreft de *opzet* de schriftelijke inlichtingen van de gemeente over de genomen beveiligingsmaatregelen. De *controle van het bestaan* gaat een stapje verder: het gaat hier om het objectief waarnemen door de auditor van de genomen maatregelen. Bij een audit op de *werking* van maatregelen is de diepgang het grootst. Het functioneren van de beveiligingsmaatregelen wordt dan beoordeeld over een bepaalde periode (dat wil zeggen de periode dat de specifieke beveiligingsmaatregel 'werkt'). Wordt dit bij een echte EDP-audit doorgaans vastgesteld door het uitvoeren van tests e.d., bij de GBA-audit is er door BPR voor gekozen om dit marginaal te toetsen. Dat betekent dat genoegen wordt genomen met rapportages van de gemeente waarbij de werking van de beveiligingsmaatregelen achteraf kan worden vastgesteld.

Het zal duidelijk zijn dat een dergelijke rapportage hiervoor dan wel geschikt moet zijn. In onderstaande figuur is dit in beeld gebracht:

Normenkader na 1 juli 2002

Naast de 'verdieping' van de audit, wordt een aantal eisen bij het procesdeel verplicht gesteld. Dit betekent dat bij niet voldoen een her-audit op de desbetreffende eis volgt.
In de tabel op de volgende pagina is een overzicht gegeven inclusief het in goed overleg met BPR afgestemde normenkader.

Nr	Onderdeel	Eis	Verplicht voor 1-7-02	Verplicht na 1-7-02	Normenkader
1	Back-up en herstel	Reconstructie voorzieningen	Gedeeltelijk	Ja	De back-up tape met GBA-gegevens zoals die 1 werkdag geleden waren, moet altijd binnen 1 werkdag kunnen worden 'gerestored'. Een en ander behoort te zijn vastgelegd in een schriftelijke procedure die jaarlijks wordt getest in eigen huis.
2		Bewaarplaats	Ja	Ja	De back-up tape met GBA gegevens moet in een beveiligde ruimte worden bewaard anders dan de computerruimte. De week*save* moet in een beveiligde ruimte in een ander gebouw worden bewaard. Doel hiervan is dat de back-up tapes beschikbaar zijn, nadat een eventuele calamiteit heeft plaatsgevonden.
3		Mutatie reconstructie	Gedeeltelijk	Ja	Er moeten voorzieningen zijn getroffen om een reconstructie van de mutaties die na de laatste back-up zijn aangebracht, te kunnen uitvoeren. Deze voorzieningen moet zijn vastgelegd in een schriftelijke procedure die jaarlijks wordt getest. Doel hierbij is het kunnen herstellen van de situatie tussen 'crash' en de laatste back-up. De test mag plaatsvinden tegelijk met de uitwijkbeproeving.
4		Verkeerde verstrekkingen	Ja	Ja	In een schriftelijke procedure moet zijn vastgelegd welke voorzieningen zijn getroffen om de gevolgen van verkeerd uitgevoerde systematische verstrekkingen ongedaan te kunnen maken. De via het GBA-netwerk verzonden systematische verstrekkingen dienen minimaal 4 dagen te worden bewaard en de via alternatieve media verzonden systematische verstrekkingen dienen minimaal 1 maand te worden bewaard.
5	Uitwijk	Uitwijkvoorzieningen	Gedeeltelijk	Ja	Er moeten voorzieningen zijn getroffen om te kunnen uitwijken, hetgeen aantoonbaar dient te zijn gemaakt door het overleggen van een schriftelijke uitwijkprocedure en een uitwijkovereenkomst met een uitwijkleverancier. Zowel het interne als externe deel van de uitwijkprocedure moet jaarlijks worden onderworpen aan een test waarbij de werking wordt vastgesteld.
6	Beveiliging	Beveiligingssysteem	Nee	Ja	Er is beleidsmatig aandacht voor de eisen die de gemeente stelt aan de exclusiviteit van de GBA en aan de wijze waarop de informatiebeveiliging wordt gerealiseerd, gecontroleerd en geëvalueerd. Daarnaast moet er een actueel beveiligingsplan GBA zijn opgesteld dat de technische en organisatorische uitwerking van het beveiligingsbeleid bevat. Daarnaast zou er sprake moeten zijn van functiescheiding in de beveiligingsorganisatie
7		Technische maatregelen	Nee	Ja (gedeeltelijk)	De gemeente heeft maatregelen van technische aard genomen om verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking van GBA gegevens tegen te gaan. Er dient sprake te zijn van een individueel bevoegdheidsprofiel en er worden een eisen gesteld aan de wachtwoorden van de tot de GBA toegang gevende informatiesystemen.
8		Organisator-ische maatregelen	Nee	Ja (gedeeltelijk)	De gemeente heeft maatregelen van organisatorische aard genomen om verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking van GBA gegevens tegen te gaan.
9		Bewerker	Nee	Ja (indien van toepassing)	Ingeval de gemeente gebruik maakt van een bewerker, dient de gemeente voorzieningen te treffen om vast te stellen en te bewaken dat de bewerker voldoet, resp. blijft voldoen aan het gestelde in en krachtens artikel 53 van het Besluit GBA.
10		Alternatieve media	Nee	Ja	De gemeente heeft in het kader van de verzending van GBA-berichten via alternatieve media dusdanige maatregelen genomen om te kunnen voldoen aan de in paragraaf 7.3.5 van het LO geldende eisen. Deze worden jaarlijks getest.
11	Privacy	Gegevensverwerking	Ja	Ja	De integriteit van de gegevens in de GBA moet in de administratieve organisatie worden gewaarborgd.
12		Gemeentelijke verordening	Ja	Ja	Er moet een GBA- privacyverordening zijn vastgesteld of een privacyverordening met een daarop gebaseerd GB -privacyreglement.
13		Naleving	Ja	Ja	De daarvoor in aanmerking komende verstrekkingen

Nr	Onderdeel	Eis	Verplicht voor 1-7-02	Verplicht na 1-7-02	Normenkader
		Protocolplicht			moeten worden geprotocolleerd.
14		Regeling hoofdlijnen beheer GBA	Ja	Ja	De hoofdlijnen van het beheer dienen schriftelijk te zijn beschreven, vastgesteld en voor een ieder ter inzage gelegd.
15		Naleving procedure inzagerecht	Nee	Nee	De burger moet de mogelijkheid hebben zijn of haar gegevens in te zien.
16		Regeling buitengemeentelijke afnemers	Ja	Ja	Het verstrekken van persoonsgegevens aan buitengemeentelijke afnemers is geregeld door het bevoegd gezag. Er is een autorisatieprocedure.
17		Regeling binnengemeentelijke afnemers	Ja	Ja	Het verstrekken van persoonsgegevens aan binnengemeentelijke afnemers is geregeld bij of krachtens gemeentelijke verordening.
18		Regeling verstrekking 'vrije derden'	Ja	Ja	Het verstrekken van persoonsgegevens aan 'vrije derden' is geregeld bij of krachtens gemeentelijke verordening.
19		Rechten van de burger	Ja	Ja	Er is een schriftelijke procedure om verzoeken om geheimhouding af te handelen.

Slot

Zoals gezegd: de GBA audit moet worden gezien als een 'groeimodel'. Dat biedt in de toekomst ruimte om ook aandacht te besteden aan andere kwaliteitsaspecten zoals het volledig zijn van de basisadministratie. Ook de actualiteit van de gegevens(mutaties) zou bij toekomstige audits kunnen worden beoordeeld via steekproeven. Zaken als versiebeheer en de recovery-aspecten van GBA II (GBA via TCP/IP met een continue berichtenverkeer) vallen vooralsnog buiten de scope van de audit. Er is nog veel werk aan de winkel. (*mij)*