RISICO'S REGISTREREN PERS

Steeds meer overheden en derden hebben toegang tot wettelijke persoonsgegevens

Hoe veilig zijn de gegevens in de gemeentelijke basisadministratie persoonsgegevens (GBA)? Professionals zijn in staat miljoenen persoonsprofielen te maken, die voor allerlei doeleinden kunnen worden gebruikt. Kees Zwinkels gaat in op de risico's en de zorgplichten van bestuursorganen. Mede in het licht van de nieuwe wet Basisregistratie Personen.

door: KEES ZWINKELS **beeld:** GETTY IMAGES

De wet gemeentelijke basisadministratie persoonsgegevens (GBA) is de basis voor het registreren van de wettelijke persoonsgegevens. Er is inmiddels op jaarbasis sprake van tientallen miljoenen transacties (nieuwe registraties, wijzigingen en raadplegingen). Steeds meer (semi-)overheden en derden hebben toegang tot de wettelijke persoonsgegevens. De vraag is wat de risico's zijn. En hoe de beveiliging van deze gegevens, vastgelegd in de huidige GBA-regelgeving, wordt gewaarborgd. Vertrekpunt is dat de persoonsgegevens privacygevoelig zijn. Daarom heeft de wet GBA het karakter van een gesloten basisregistratie. Alleen de bestuursorganen (krachtens publiek recht ingesteld of met openbaar gezag bekleed) en de derden, die wettelijke of overheidstaken uitvoeren, kunnen de gegevens raadplegen via de landelijke databases.
De huidige wet zal worden opgevolgd door de wet Basisregistratie Personen. Het wetsontwerp is in april 2012 ingediend.

Risico's

Om de risico's te illustreren schets ik een voorbeeld. Professionals, werkzaam bij gemeenten, hebben via het landelijke Suwinetwerk per bijstandscliënt toegang tot de GBA-gegevens, de gegevens van de sociale diensten en tot die van landelijk opererende publieke dienstverleners (bijvoorbeeld het UWV, de Rijksdienst voor het Wegverkeer, de belastingdienst en de kamers van koophandel). De professionals zijn derhalve in staat profielen van hun cliënten aan te maken. Afhankelijk van hun behoeften kiezen de medewerkers voor meer of minder diepgang per profiel. Staatssecretaris de Krom (inmiddels demissionair) heeft per brief de 100.000-plusgemeenten gevraagd nog eens kritisch naar hun informatiebeveiliging te kijken in relatie tot het gebruik van het Suwi-netwerk.
Te constateren is dat de beschikbaarheid van de GBA-gegevens en overige publieke persoonsgegevens per burger zal leiden tot de aanmaak van miljoenen persoonsprofielen. Relevant hierbij is de snelle toename van koppelingen tussen de overheidsdatabases binnen Nederland en binnenkort over de grenzen heen.
De profielinformatie wordt steeds meer ingezet om overheidstaken efficiënter te vervullen. In hoeverre is deze informatie gemakkelijk toegankelijk en bewerkbaar? In hoeverre hebben bijvoorbeeld de medewerkers bij overheden en derden toegang tot de GBA-gegevens van inmiddels tienduizenden beveiligde personen in Nederland?
Een tweede categorie van risico's zijn de afwijkingen tussen de officiële GBA-gegevens en de persoonsgegevens in de registraties van (semi-)overheden en de derden. Neemt het aantal schaduwadministraties met afwijkende persoonsgegevens bij de niet-gemeenten daadwerkelijk af?
Last but not least heeft de Diginotar-affaire ons duidelijk gemaakt dat de risico's ook van buiten komen. Er was sprake van een digitale inbraak bij deze voor de overheid relevante en onbeveiligde certificatiedienstverlener.

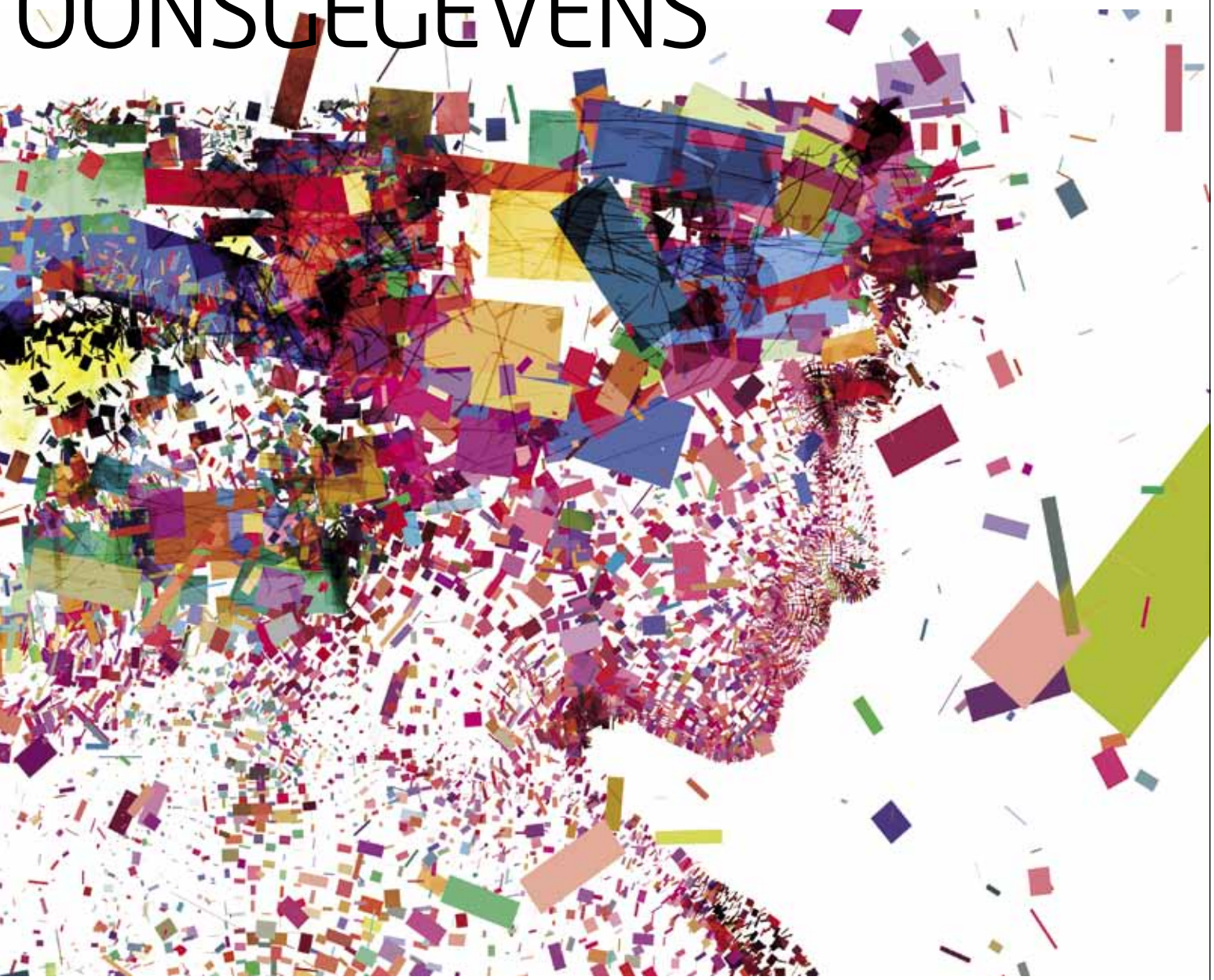
Maatregelen

De bestuursorganen hebben een gebruiksplicht met betrekking tot de wettelijke persoonsgegevens. Aanvullend is er de terugmeldingsplicht wanneer in een concrete situatie twijfel bestaat over de juistheid van de geregistreerde persoonsgegevens. Het sluitstuk is de onderzoeksplicht voor gemeenten naar aanleiding van de terugmeldingen.
Deze drie verplichtingen hebben het karakter van zorgplichten. Zij zijn algemeen geformuleerd, de uitvoering is op diverse wijzen mogelijk. Er is geen ruimte meer voor detailvoorschriften. Immers, de wetgever kan de snelle ICT-ontwikkelingen niet bijhouden. Daarom worden in de nieuwe wet voor de basisregistratie personen de hierboven genoemde zorgplichten aangevuld met globale voorschriften over wie voor wat verantwoordelijk is met betrekking tot de inrichting, het beheer en de beveiliging van de ICT-voorzieningen (de landelijke databases en het beveiligde netwerk). Het agentschap Basisregistratie Personen blijft in de nieuwe wet namens het ministerie BZK de beheerder van de landelijke voorzieningen (LV's). De hierboven genoemde bestuursorganen en de derden zijn verantwoordelijk voor de aansluiting van hun eigen ICT-voorzieningen op de LV's. De genoemde verantwoordelijkheden voor de ICT-voorzieningen zou ik ook willen typeren als zorgplichten. Omdat de zorgplichten algemeen zijn geformuleerd neemt de relevantie toe van wat BZK, het agentschap, de bestuursorganen en derden concreet met elkaar en op basis van overeenkomsten en servicenormen afspreken over de beveiliging van de persoonsgegevens. En hoe zij daarmee omgaan in de praktijk. Helaas geven

WET BASISREGISTRATIE PERSONEN

De positie van het wetsontwerp Basisregistratie Personen zal na de aankomende verkiezingen weer opnieuw worden bepaald. Hoe dan ook: de nieuwe wet zal een centrale positie in het stelsel van basisregistraties innemen. Aanvullend op de hier beschreven zorgplichten krijgen de landelijke ICT-voorzieningen grote betekenis. De inrichting en het beheer daarvan zullen geen onderwerp van wettelijke voorschriften meer zijn. De wet zal slechts uitspraken doen over wie voor welke gegevens en wanneer verantwoordelijk is, inclusief de koppelingen met bestanden elders.
De mogelijke roep van het parlement om wederom de heilloze weg van gedetailleerde ICT-voorschriften op te gaan, kan slechts voorkomen worden indien over de beveiliging van persoonsgegevens helder en frequent wordt gerapporteerd op basis van de gekozen doelstellingen.

OONSGEGEVENS



Voor reacties en nieuwe bijdragen van IT-experts: Henk Ester, 070 3780397 h.ester@sdu.nl

de beschikbare rapportages weinig of geen inzicht in de beschreven risico's en de uitvoering van de bijpassende maatregelen. Dit, ondanks het feit dat het parlement hier regelmatig om vraagt.

Beveiligingsnormen

Aanvullend op de GBA-auditnorm voor gemeenten op grond van de wet GBA is er recentelijk de norm ICT-beveiligingsassessments DigiD bijgekomen. De norm bevat elementen die terug te vinden zijn in de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum. Onderwerpen zijn onder andere de toegangsbeveiliging, de afspraken met leveranciers, securityscans en penetratietesten. Gemeenten zijn ook begonnen met het invoeren van maatregelen op grond van de Code voor informatiebeveiliging (ISO/NEN 27001). Deze code omvat niet minder dan honderdvijfentwintig uit te voeren maatregelen.
Het gebruik van de beveiligingsnormen geeft aanleiding tot een aantal vragen. Allereerst doen de normen geen uitspraken over de na te streven beveiligingsniveaus, maar slechts over de typen maatregelen. Het bekende artikel 13 Wet bescherming persoonsgegevens geeft richting voor hoe te handelen. Degene die verantwoordelijk is voor de verwerking van persoonsgegevens, neemt organisatorische en technische maatregelen om een passend beveiligingsniveau te garanderen, gelet op de aanwezige risico's voortvloeiende uit de verwerking en de aard van de te beschermen gegevens. Een bestuursorgaan of derde die maatregelen neemt, moet dus inzicht geven in het gekozen niveau van beveiliging op basis van een expliciete en heldere risico-analyse. De wetgever kan de bestuursorganen en derden nog een duwtje in de richting van een actievere opstelling geven door expliciet vast te leggen in hoeverre er op basis van de specifieke beveiligingsnormen gehandhaafd kan worden.

Kosten

Een tweede vraagstuk betreft de te maken kosten per organisatie met betrekking tot de toe te passen beveiligingsnormen en maatregelen. Ik heb hierboven reeds drie normen genoemd. Ook binnen het kader van de uitvoering van de Suwi-regelgeving is beveiliging een onderwerp van aandacht. En last but not least spreken de externe accountants zich uit over informatiebeveiliging bij het jaarlijks beoordelen van de doelmatigheid en rechtmatigheid binnen de overheid. Beveiliging van de wettelijke en overige privacygevoelige persoonsgegevens is derhalve het onderwerp van een groeiend aantal los van elkaar staande audits en assessments. Het verdient aanbeveling om te gaan werken met één gestandaardiseerde basisaudit, gericht op het toetsen van de beveiliging van de persoonsgegevens per organisatie op grond van de van toepassing zijnde regelgeving en normen. Deze integrale aanpak leidt tot een kostenbesparing en tot een vergelijking van de auditresultaten tussen de bestuursorganen en derden onderling. BZK kan een voortrekkersrol vervullen. Immers, de huidige GBA-audit met aandacht voor privacy en beveiliging gaat omgezet worden in een zelfevaluatie voor gemeenten in de nieuwe wet basisregistratie personen. Kan het model voor zelfevaluatie de basis zijn voor de na te streven basisaudit voor beveiliging?
Kortom, de risico's met betrekking tot de beveiliging van persoonsgegevens nemen toe. Een belangrijk voorbeeld is de snelle groei van burgerprofielen. Uitgaande van de politieke verantwoordelijkheid, van toepassing op de bestuursorganen en derden, is het logisch dat zij regelmatig uitleg geven over de stand van zaken met betrekking tot de beveiliging van de verwerkte persoonsgegevens. Bestuursorganen en derden zullen op grond van risico-analyses inzicht moeten geven in de gekozen beveiligingsniveaus en de getroffen maatregelen. Het verdient aanbeveling om te werken met een gestandaardiseerde basisaudit voor beveiliging. BZK kan op basis van de gegevens van bestuursorganen en derden regelmatig rapporteren over de risico's en de maatregelen. «

Kees Zwinkels (c.zwinkels@vu.nl) is als docent-onderzoeker verbonden aan de Vrije Universiteit Amsterdam, vakgebied Recht en e-overheid. Daarnaast is hij werkzaam bij DeClercq Advocaten • Notarissen.