>>>Quickscan

- OVERHEID
- BURGER
- BELANGEN
- RISICO'S
- TOEKOMSTVASTHEID

Privacy is verantwoordelijkheid van informatiemanager

Burgers maken zich in toenemende mate zorgen over hun privacy. Hierdoor komt er steeds meer aandacht voor dit onderwerp vanuit verschillende hoeken. Ook in het conceptreageerakkoord van VVD-CDA is het onderwerp expliciet benoemd. Door de verregaande digitalisering van onze informatiemaatschappij kunnen steeds meer gegevens van burgers worden opgeslagen en voor andere doeleinden worden gebruikt dan oorspronkelijk de bedoeling was. Zonder het nemen van de juiste maatregelen wordt de privacy van het individu te veel aangetast. Volgens de auteurs van dit artikel dient de informatiemanager een grotere rol te spelen bij het borgen van de privacy van burgers.

Tekst **Christ Reniers en Dennis Baaten**

De overheid en het bedrijfsleven bouwen informatiesystemen waarin persoonsgegevens van burgers worden verwerkt. In hun ijver om hun dienstverlening te optimaliseren, verzamelen ze zoveel mogelijk informatie en zoeken ze de grenzen op van wat in hun ogen acceptabel is. Hierbij wordt weinig tot geen rekening gehouden met het privacybelang van burgers. Bovendien lopen de meningen tussen burgers en organisaties over wat acceptabel is nogal uiteen – dat is ook nergens duidelijk vastgelegd. Het leidt vaak tot verhitte publieke discussies, zoals het geval was bij de invoering van de OV-chipkaart, rekeningrijden, het centraal opslaan van vingerafdrukken buiten het paspoort, en slimme energiemeters. Vaak is de weerstand van burgers terug te voeren op het bezwaar dat organisaties deze gegevens in de toekomst kunnen gebruiken voor toepassingen waar ze oorspronkelijk niet voor bedoeld waren; het zogenaamde Big Brother-effect.
In het geval van de OV-chipkaart slaan de vervoersbedrijven vervoersgegevens van de individuele reiziger op voor marketingdoeleinden, terwijl dat voor het doel 'reizen met het openbaar vervoer' niet nodig is. Dat is volgens het College bescherming persoonsgegevens verboden. Rekeningrijden stelt de overheid in staat om zeer nauwkeurig te bepalen welke auto op welk moment waar aanwezig was; een handig instrument voor bijvoorbeeld opsporingsdiensten. Uit een onderzoek van studenten aan de Universiteit van Amsterdam blijkt dat slimme energiemeters zeer gedetailleerde informatie over het leefpatroon van burgers geven. Zo is aan het verband tussen gas- en waterverbruik exact te zien hoe lang en op welke temperatuur er is gedoucht, maar ook of iemand alleen woont en bezoek krijgt. Daarnaast laat het verschil in gas- of elektriciteitverbruik zien of iemand zelf heeft gekookt of een magnetronmaaltijd heeft genuttigd.

GEBREK AAN VERTROUWEN

Zulke voorbeelden zorgen ervoor dat privacy in toenemende mate wordt gebruikt als argument tegen grootschalige informatisering- en digitaliseringtrajecten. Met name de Nederlandse overheid heeft hier veel last van. Door in het verleden gemaakte fouten is het vertrouwen van burgers in de overheid laag. Onvoldoende borging of bescherming van de privacy is dan ook een veelgehoorde reden om de hakken in het zand te zetten. Feit is echter dat burgers en hun overheid nu eenmaal op elkaar zijn aangewezen. Overstappen op een andere overheid is geen optie. Daarom wordt het tijd dat de overheid het privacybelang van burgers centraal gaat stellen. De informatiemanager kan een grote rol spelen in het beschermen van de privacy van burgers.

JURIDISCHE BENADERING

Op dit moment wordt privacy bij ontwikkeltrajecten van de overheid vaak juridisch aangevlogen. In de praktijk betekent dit dat er voor privacy alleen eisen worden gesteld vanuit wet- en regelgeving. Dit is een goede zaak, maar biedt onvoldoende zekerheid voor de meeste ontwikkeltrajecten. De wetgeving in Nederland stelt namelijk algemene kaders en is niet tot in detail uitgewerkt. Hierdoor ontstaat er ruimte voor verschillende interpretaties en is het moeilijk om te bepalen of iets in een informatiseringstraject wel of niet mag.
Nu verbieden dat bepaalde gegevens in een gegevensverzameling worden gebruikt, biedt geen garantie dat dit in de toekomst ook niet zal gebeuren. Er is namelijk niemand die kan garanderen dat de wetten die misbruik van gegevens dienen te voorkomen, er over een aantal jaren nog zijn. Daarnaast blijft de verleiding om de verzamelde gegevens toe te passen voor andere doeleinden groot.

SYSTEEMONTWERP

Beter is om bij het ontwerp van informatiesystemen al uit te gaan van een minimale set van gegevens. Op deze manier kunnen organisaties in de toekomst ook niet in de verleiding komen om gegevens voor andere doeleinden te gebruiken, en is het beschermen van privacy minder afhankelijk van wet- en regelgeving. Dit is niet alleen in het belang van burgers, maar ook in het belang van organisaties; deze kunnen namelijk aansprakelijk worden gesteld

HET ONTWERP VAN INFORMATIE-SYSTEMEN DIENT AL UIT TE GAAN VAN EEN MINIMALE SET VAN GEGEVENS

voor het lekken (per ongeluk of door inbraak) van persoonsgegevens. Kortom, een optimale borging van de privacy is goed voor iedereen: hoe minder vastlegging en uitwisseling van gegevens, hoe beter.

SLEUTELROL INFORMATIEMANAGERS

Hier komt de taak van informatiemanagers in beeld. Informatiemanagers zijn verantwoordelijk voor het informatiebeleid binnen een organisatie. Deze positie (aan de kant van de business) maakt informatiemanagers bij uitstek geschikt om een sleutelrol te vervullen bij het borgen van de privacy. Informatiemanagers dienen erop toe te zien dat organisatiedoelen worden bereikt door een minimale en zo anoniem mogelijke vastlegging en uitwisseling van persoonsgegevens. Zo is het bijvoorbeeld bij het kopen van een pakje sigaretten helemaal niet nodig om het BSN, de geboortedatum, of andere identificerende gegevens af te geven. Het enige wat de verkoper moet weten is een simpel 'ja' of 'nee' op de vraag of de koper ouder is dan 16 jaar. Het is aan de informatiemanager om vanuit de businesseisen en/of -wensen te formuleren met betrekking tot het beschermen van privacygevoelige gegevens binnen de informatievoorziening. Vervolgens is het aan informatiearchitecten om binnen de gestelde kaders te komen tot creatieve oplossingen. Niet alleen het belang van opdrachtgevers, maar ook het belang van burgers dient expliciet te worden meegenomen in het informatiebeleid van een organisatie.
Dit betekent dat de informatiemanager rekening moet houden met de privacywet- en -regelgeving en door middel van beleid moet aansturen op het gebruiken van een minimale set van gegevens van burgers in de informatievoorziening. Op die manier worden niet alleen het belang en de rechten van burgers centraal gesteld, maar worden de (aansprakelijkheids)-risico's voor de organisatie als gevolg van datalekken beperkt.

PRIVACYBELANG NIET CENTRAAL

Momenteel gebeurt dat nog veel te weinig. Vaak wordt uitgegaan van een zo groot mogelijke (standaard)gegevensset, omdat dit de meeste flexibiliteit richting de toekomst lijkt te bieden. Het informatiebeleid stelt in zo'n geval het belang van de organisatie centraal. Dit lijkt vrij logisch, maar met name bij overheidsorganisaties is er hier toch iets vreemds aan de hand. Een overheidspartij is vaak ook de beheerder van de gegevens die uiteindelijk in het systeem terechtkomen, en dus verantwoordelijk voor de bescherming van de persoonsgegevens die betrekking hebben op burgers. Met een risicoanalyse definieert een overheidspartij een afgewogen set van maatregelen om de persoonsgegevens van burgers te beschermen. In de meeste gevallen zijn economische motieven de basis voor deze afweging, ofwel: wat zijn de kosten voor het invoeren van bepaalde maatregelen en wat is de mogelijke schade indien deze maatregelen niet worden getroffen? De overheidspartij bepaalt dus ook of het risico van burgers acceptabel is. Dit lijkt te impliceren dat de overheidspartij het privacybelang van burgers vooropstelt, maar dat is bijna nooit het geval.

CONCLUSIE

Daarom is het belangrijk dat de belangen van alle belanghebbenden in het informatiebeleid worden meegenomen om op die manier tot een betere bescherming van een ieders privacy te komen. De informatiemanager stelt eisen aan de informatiseringsoplossing vanuit de business waarbij tevens het privacybelang van burgers centraal staat; minimale uitwisseling en vastlegging van persoonsgegevens is hierbij het uitgangspunt. Op deze manier is de toekomstvastheid van informatiesystemen in relatie tot privacy van burgers zo hoog mogelijk. De informatiemanager heeft daarmee een belangrijke taak in de bescherming van privacy van burgers. ✖

Christ Reniers en Dennis Baaten zijn werkzaam bij Verdonck, Klooster & Associates.

HET BELANG VAN BURGERS MOET WORDEN MEEGENOMEN IN HET INFORMATIEBELEID