Vereniging van
Nederlandse Gemeenten

Informatieveiligheid, randvoorwaarde voor de professionele gemeente

Pre-ambule

Gemeenten zijn voor steeds meer beleidsterreinen verantwoordelijk. Zij maken daarbij gebruik van de mogelijkheden van informatie-uitwisseling. Door informatie te delen en processen te optimaliseren kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van burgers verbeteren en meer mensen aan het werk krijgen. Ook voor de decentralisatie van taken op gebied van werk, jeugdzorg en AWBZ zullen gemeenten onderling en met diverse ketenpartners informatie uitwisselen.

Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie professioneel organiseren. Informatie moet immers beschikbaar en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten voldoende rekening houden met beveiligings- en privacyaspecten.

Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie?

In de kern raakt informatievoorziening en -veiligheid de legitimatie van het werk van de gemeentelijke bestuurders. Het is namelijk niet alleen een technische vraag maar ook een politieke en bestuurlijke. Het raakt de bedrijfsvoering van de gemeente en vraagt daarom om een bestuurlijke visie, focus en draagvlak. Om informatieveiligheid te garanderen zal iedere gemeentelijke organisatie daarom actie moeten ondernemen. Zowel technisch als organisatorisch.

Gemeenten willen een krachtig geluid afgeven en verklaren dat zij de verantwoordelijkheid voor informatieveiligheid (verder) op zich nemen. Zij willen tevens een logisch en noodzakelijk vervolg geven aan de stappen die de Nederlandse gemeenten al eerder hebben genomen zoals de oprichting van de Informatiebeveiligingsdienst voor gemeenten (IBD). Deze IBD is, na verkregen instemming tijdens de BALV van september 2012, sinds 1 januari 2013 in opdracht van de VNG operationeel als onderdeel van KING en heeft als kerntaak gemeenten op het gebied van informatieveiligheid met een breed palet te ondersteunen.

Gemeenten willen, met oog voor ieders positie, verder invulling geven aan lokaal informatieveiligheidsbeleid en dat zowel bestuurlijk als ambtelijk in de organisatie borgen. Dat vergt continue alertheid en het leren van ervaringen. Daarbij willen zij transparant zijn over de staat van de informatieveiligheid: in de eerste plaats horizontaal, maar ook in de richting van de (keten)partners.

RESOLUTIE

De leden van de VNG in de BALV bijeen op 29 november 2013 te Utrecht komen overeen,

Constaterende dat

- Gemeenten beseffen dat de risico's van informatieveiligheid manifest zijn.
- Een professionele gemeente ook informatieveiligheid professioneel heeft ingericht.

Overwegende dat

1. Gemeenten verantwoordelijk zijn voor informatieveiligheid bij het vervullen van maatschappelijke taken richting burgers en bedrijven.
2. Gemeenten een verantwoordelijkheid hebben voor informatieveiligheid in hun rol als partner binnen (overheids) ketens. De rol - en daarmee de verantwoordelijkheid - van de gemeente, varieert van eigenaar, tot leverancier en/of afnemer van gegevens.
3. Gemeenten samenwerken op het gebied van informatieveiligheid.

Instemmende dat

1. Informatieveiligheid onderdeel wordt van collegeambities 2014-2018 en opgenomen wordt in de portefeuille van een van de leden van het college van B&W.
2. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.
3. Gemeenten de Baseline Informatiebeveiliging Gemeenten vaststellen als hét gemeentelijke basisnormenkader voor informatieveiligheid.
4. Gemeenten informatieveiligheidsbeleid vaststellen aan de hand van de Baseline Informatiebeveiliging Gemeenten. Uitvoering van dat beleid wordt gebaseerd op eigenstandige risicoafwegingen. Gemeenten zijn zich daarbij bewust van de (continu veranderende) informatieveiligheidsrisico's die ze lopen en nemen hierop adequate maatregelen.
5. Gemeenten informatieveiligheid bestuurlijk en organisatorisch borgen door aansluiting in de reeds bestaande planning- en controlcyclus. Gemeenten creëren hiernaast, door middel van leren en ontwikkelen, blijvend bewustzijn op informatieveiligheid.
6. Gemeenten de lokale invulling rondom het thema van informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners. Deze transparantie wordt ondermeer behaald door gebruik te maken van waarstaatjegemeente.nl. Deze openbare informatie vormt de basis voor jaarlijkse collegiale beoordeling (peer reviews). Daarnaast toetst een interbestuurlijke visitatiecommissie, tenminste eens in de vijf jaar, of het systeem van 'verplichtende zelfregulering' voldoende werkt. Informatie over gemeentelijke informatieveiligheid is alleen openbaar in de vorm van metadata over de gemeentelijke keten. Gemeentelijke kwetsbaarheden, specifieke maatregelen en auditrapportages zijn niet openbaar.

Dragen het bestuur van de VNG op om bij het Rijk en ketenpartners te bewerkstelligen dat

1. De BIG als basisnormenkader voor het gemeentelijke domein wordt erkend.
2. De minister van BZK zorgt voor hergebruik van bestaande informatie en beperking van audit- en monitorlast. Hierbij is het principe van Single Information Single Audit het uitgangspunt.
3. Gemeenten voldoende tijd krijgen voor een gefaseerde en gedifferentieerde implementatie van informatieveiligheid die gebaseerd is op lokale afwegingen en financieringsmogelijkheden.
4. Helderheid komt over een voor gemeenten werkbare meldplicht bij datalekken.
5. Een externe adviserende (interbestuurlijke) visitatiecommissie wordt ingericht, gefinancierd door het Rijk.
6. Wet- en regelgeving zo beperkt mogelijk wordt gehouden.

En dragen de VNG verder op om

1. De doorontwikkeling van de BIG organisatorisch te borgen.
2. Samen met het Rijk, ketenpartners en KING te verkennen hoe leveranciers beter kunnen worden betrokken bij het borgen van informatieveiligheid.
3. Individuele gemeenten te blijven aansporen tot het instellen van een lokaal informatieveiligheidsbeleid.