Vereniging van
Nederlandse Gemeenten

# Informatieveiligheid, randvoorwaarde voor de professionele gemeente

## Toelichting

Gemeenten zijn voor steeds meer beleidsterreinen verantwoordelijk. In vrijwel alle gevallen wordt daarbij gebruik gemaakt 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 is het noodzakelijk dat gemeenten ook de beveiliging van informatie professioneel organiseren. Informatie moet immers beschikbaar en integer (lees: betrouwbaar) zijn en mag alleen door bevoegden zijn in te zien (vertrouwelijk). 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? Wat betekent het bijvoorbeeld als informatie niet beschikbaar of betrouwbaar is, of in de verkeerde handen is gekomen?

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

Los van het feit dat menig gemeente al vergevorderd is in de professionalisering van informatieveiligheidsbeleid willen gemeenten een krachtig geluid afgeven en verklaren dat zij de verantwoordelijkheid voor informatieveiligheid (verder) op zich nemen. Dit doen ze met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente". Hiermee nemen gemeenten verantwoordelijkheid voor het opstellen, uitvoeren en handhaven van de voorwaarden voor informatieveiligheid.

Met de resolutie geven gemeenten een logisch en noodzakelijk vervolg aan de stappen die al eerder zijn gezet, zoals de oprichting van de Informatiebeveiligingsdienst voor gemeenten (IBD). Tijdens de BALV van september 2012 is ingestemd met de oprichting van de IBD. Sinds 1 januari 2013 is de IBD 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.

In deze toelichting worden achtereenvolgens de punten uitgewerkt die in overweging worden genomen. Vervolgens worden de punten beschreven waar gemeenten met deze resolutie mee instemmen. Daarna worden de punten uitgediept die de gemeenten middels de resolutie terugvragen van Rijk en ketenpartners. Tot slot volgen de punten waar de leden de VNG toe opdragen. Bij alle uitwerkingen wordt eerst de oorspronkelijke tekst zoals deze ook in de resolutie staat beschreven, zodat de relatie tussen de resolutie en deze toelichting helder is.

## Overwegende dat

1. ***Gemeenten verantwoordelijk zijn voor informatieveiligheid bij het vervullen van maatschappelijke taken richting burgers en bedrijven.***

Gemeenten beschikken over uiterst gevoelige informatie van burgers: gegevens over onder meer hun inkomen, hun relaties, hun sociale positie, en hun gezondheidstoestand. De gemeente heeft de wettelijke en morele plicht om daar uiterst zorgvuldig mee om te gaan. Burgers en bedrijven verwachten dit en moeten hierop kunnen vertrouwen. Deze verantwoordelijkheid kan niet worden overgeheveld naar bijvoorbeeld softwareleveranciers of ketenpartners. Door middel van deze resolutie bekrachtigen de gemeenten deze verantwoordelijkheid.

Gemeenten maken deel uit van Veiligheidsregio's, Regionale Uitvoeringsdiensten (RUD's), Gemeentelijke of Gemeenschappelijke Gezondheidsdiensten (GGD's), maar ook Shared Service Organisaties. Ook deze organisaties kunnen beschikking hebben over gevoelige informatie. Gemeenten hebben daarom naast een lokale verantwoordelijkheid een rol op (boven)regionaal vlak.

Gemeenten hebben individueel en als collectief een verantwoordelijkheid om de informatie(stromen) op de juiste manier te beveiligen. Het is hierbij van belang dat binnen dit verband duidelijk is wie verantwoordelijk is voor informatieveiligheid en welke eisen de gezamenlijke gemeenten aan het verlengde lokaal bestuur stelt. Bijvoorbeeld door het onderdeel te laten zijn van contractafspraken of door het beschrijven van de eisen in een gemeenschappelijke regeling.

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.***

Gemeenten maken onderdeel uit van een veelheid aan ketens. Voorbeelden hiervan zijn de GBA-keten, de SUWI-keten of de keten bij het Omgevingsloket. De rol van de gemeente is per ketenproces verschillend. In alle gevallen heeft de gemeente echter minimaal een medeverantwoordelijkheid voor informatiebeveiliging, en in veel processen – processen waarover gemeenten de regie voeren, of waarvoor zij opdrachtgever zijn – zelfs een algehele verantwoordelijkheid.

Gemeenten nemen hun verantwoordelijkheid op het gebied van informatieveiligheid in de ketens, zodat ketenpartners op gemeenten kunnen vertrouwen. Gemeenten verwachten dezelfde houding terug van hun ketenpartners. Per keten moeten daarom afspraken gemaakt worden over aspecten als governance, risico's binnen de keten en wederzijdse transparantie.

De verantwoordelijkheid die partners in ketens hebben, bestaat uit het signaleren van en wijzen op mogelijk noodzakelijke verbeteringen van de informatieveiligheid. Ook waar gemeenten geen formele zeggenschap over een keten hebben komen zij in het algemene belang van burgers en bedrijven op voor het belang van informatieveiligheid.
Van gemeenten mag echter niet worden verwacht dat zij de verantwoordelijkheid voor informatieveiligheid van ketenpartners overnemen. Evenmin kunnen gemeenten de verantwoordelijkheid voor de eigen informatieveiligheid naar ketenpartners of bijvoorbeeld softwareleveranciers overhevelen.

3. ***Gemeenten samenwerken op het gebied van informatieveiligheid.***

Gemeenten hebben elk een actieve rol in de stelselverantwoordelijkheid voor informatiebeveiliging en kunnen als collectief informatieveiligheid naar een hoger plan tillen. Het is voor iedere gemeente van belang dat alle gemeenten een betrouwbare partner zijn.

Door middel van transparantie kunnen gemeenten van elkaar leren via best practices en kruisbestuiving. Onder andere peer reviews in de verschillende regio's faciliteren deze benodigde samenwerking.

Verder kunnen goede voorbeelden gedeeld worden via landelijke platforms, waaronder de IBD. Gemeenten hebben in dit kader niet alleen de verantwoordelijkheid om hun interne processen af te stemmen op de dienstverlening van de IBD, maar ook om informatiebeveiligingsincidenten te melden bij de IBD. Daarnaast sluiten gemeenten organisatorisch aan bij de IBD. Hiermee wordt de gemeente snel geïnformeerd en geadviseerd bij eventuele acute en/of kritische veiligheidsincidenten in een van de gemeentelijke systemen.

Naast het op orde brengen van de interne organisatie is daarom ook goede regie op softwareleveranciers noodzakelijk voor verankering van informatiebeveiliging. Gemeenten zullen als opdrachtgevers de krachten bij de aansturing van software- of hostingleveranciers en (externe) beheerorganisaties hiervoor zoveel mogelijk bundelen.

## Gemeenten stemmen er mee in 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.***

Informatie is, evenals financiën en personeel, een essentieel bedrijfsmiddel. Burgers en (keten)partners mogen van de gemeente, als professionele organisatie, verwachten dat zij uiterst zorgvuldig met informatie omgaat, de gegevens moeten goed beschermd worden. Gebeurt dit onvoldoende dan bestaat het risico op het verlies van publiek vertrouwen, aantasting van privacy, fraude, vermindering van productiviteit van de organisatie, onvoorziene kosten, verlies van inkomsten en/of imagoschade. De gevolgen hiervan kunnen van dergelijke omvang zijn dat deze bestuurlijke aandacht vereisen. Het vertrouwen van burgers in de overheid is immers in het geding.

Sturing op informatieveiligheid vanuit bestuur en topmanagement is daarom onlosmakelijk verbonden met de organisatiesturing. Het bestuur stelt de gemeentelijke organisatie in staat om aan informatieveiligheid te werken. Lokaal wijst het college van B&W verantwoordelijkheid een lid aan dat verantwoordelijk is voor informatieveiligheid.

Deze verantwoordelijkheid moet ook op de juiste plaats worden belegd in de organisatie. Hiervoor zal in de eerste plaats de gemeentesecretaris moeten worden benoemd als ambtelijk verantwoordelijke voor informatieveiligheid. Dit alles leidt tot duurzame bestuurlijke en organisatorische verankering van de verantwoordelijkheid voor informatieveiligheid.

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.***

Informatieveiligheid verdient continue aandacht. De afgelopen jaren zijn gekenmerkt door diverse incidenten zoals Diginotar, Lektober, Dorifel/Citadel en Pobelka, maar ook door het onbedoeld openbaar worden van vertrouwelijke informatie door medewerkers/ambtenaren. Ook in de toekomst moeten gemeenten waakzaam blijven voor eventuele nieuwe bedreigingen. Hiervoor is het van belang dat processen adequaat worden ingericht om informatieveiligheid te borgen. Bovendien moet het bewustzijn van informatieveiligheid van gemeentelijke medewerkers op alle niveaus worden vergroot.

Middels een aparte paragraaf in het jaarverslag informeert het college van B&W de gemeenteraad over informatieveiligheid en de dat jaar ondernomen acties.

3. ***Gemeenten de Baseline Informatiebeveiliging Gemeenten vaststellen als hét gemeentelijke basisnormenkader voor informatieveiligheid.***

Gemeenten zijn, net als alle andere organisaties, kwetsbaar als het gaat om (digitale) dienstverlening. De IBD heeft in opdracht van de VNG de Baseline Informatiebeveiliging Gemeenten (BIG) ontwikkeld. De BIG is een praktische handreiking waarin een vertaling naar de gemeentelijke organisatie is gemaakt van geldende ISO normen – door het College Standaardisatie vastgesteld als 'past-toe-of-leg-uit' normen voor de gehele overheid – en bestaande wet en regelgeving.

Gemeenten hebben met de BIG een instrument in handen waarmee zij in staat zijn om te meten of de organisatie minimaal voldoet aan normen en wettelijke voorschriften op gebied van informatieveiligheid. Gemeenten kunnen de BIG en onderliggende producten verder gebruiken om de basis op orde te brengen.

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.***

Aan de hand van de BIG stelt iedere gemeente informatieveiligheidsbeleid vast. Het college van B&W maakt hiervoor een inschatting van de risico's die de gemeente loopt. De gemeente controleert of al wordt voldaan aan de BIG met behulp van een nulmeting. Het resultaat van deze analyse geeft het verschil weer tussen het bestaande en het gewenste niveau van de gemeentelijke informatieveiligheid. Dit is de input voor de vervolgstap; het maken van een realistische planning. Hiervoor baseert het college van B&W zich op de algemene (financiële) uitgangspunten die de gemeenteraad stelt.

Een realistische planning is belangrijk om beweging te krijgen en te houden, maar ook om de juiste mensen en de juiste middelen op de juiste tijd te kunnen inzetten. Deze planning wordt gemaakt op basis van wat de risico's zijn bij het ontbreken van de maatregel en welke kosten er aan de invoering verbonden zijn. Het gemeentebestuur geeft richting door te kiezen voor een top-X van maatregelen en zal deze als eerste implementeren.

Een voorbeeld van een maatregel is het beleggen van de functierol Chief Information Security Officer (CISO) binnen de gemeente. Deze treedt op als adviseur van de portefeuillehouder en deze heeft centraal regie over het uit te voeren beleid en moet daarom een onafhankelijke taak krijgen binnen de gemeente.

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.***

Het bereiken van volwassenheid op informatieveiligheid is een geleidelijk proces waarbij de lat steeds een stukje hoger komt te liggen. Hiervoor is de 0-meting van de informatieveiligheid in gemeenten de startsituatie waar vanuit gewerkt wordt. Informatieveiligheid wordt organisatorisch geborgd in de reguliere planning- en controlcyclus.

Specifiek wordt ingezet op leren, stimuleren en kennisdelen. Gemeenten zorgen voor bewustzijn, voldoende kennis en vaardigheden bij alle medewerkers in de organisatie door periodiek op het gebied van informatieveiligheid te trainen via workshops, oefeningen en bewustwordingscampagnes.

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.***

Gemeenten hebben de verantwoordelijkheid om transparant en aanspreekbaar te zijn naar burgers bedrijven en (keten-)partners. De transparantie in het kader van zelfregulering informatieveiligheid wordt verkregen in onderstaande drie stappen die gepaard gaan met het groeipad dat gemeenten doorlopen op gebied van informatieveiligheid.

Ten eerste nemen gemeenten hun eigen verantwoordelijkheid door transparantie van college van B&W naar gemeenteraad. De transparantie richting de gemeenteraad krijgt vorm middels een aparte

paragraaf in het jaarverslag. De transparantie die via het jaarverslag gegeven wordt, biedt ook inzicht aan burgers en bedrijven.
Ten tweede betrachten gemeenten transparantie in de staat van de informatieveiligheid richting ketenpartners en Rijk. De website van waarstaatjegemeente.nl is hiervoor het instrument bij uitstek. De volgende vragen geven een indicatie van wat op waarstaatjegemeente.nl kan worden gepubliceerd:

1. Heeft de gemeente informatieveiligheidsbeleid vastgesteld?
2. Is het informatieveiligheidsbeleid van de gemeente gebaseerd op de Baseline Informatiebeveiliging Gemeenten?
3. Heeft de gemeente een top-X maatregelen die zullen worden geïmplementeerd benoemd?

Hierbij wordt aangesloten op het abstractieniveau dat ook wordt gebruikt voor rapportage richting de gemeenteraad. In 2014 worden deze vragen samen met gemeenten nader uitgewerkt. Op basis van deze informatie werken gemeenten met jaarlijkse peer reviews. Hiermee helpen gemeenten elkaar verder door middel van collegiale toetsing.

Als laatste stap zien gemeenten een in te richten onafhankelijke interbestuurlijke visitatiecommissie. Deze commissie zal gemeenten op bestuurlijk niveau adviseren over informatieveiligheid. De visitatiecommissie is hiermee geen klassieke toezichthouder, maar vooral een bestuurlijk 'leerinstrument'. De commissie kan zich bij de selectie van gemeenten baseren op de beschikbare monitorinformatie van waarstaatjegemeente.nl, maar bezoekt iedere gemeente minstens één keer per 5 jaar. De visitatiecommissie zal zijn resultaten over de werking van het systeem van verplichtende zelfregulering rapporteren aan een, nog in te stellen, hoog ambtelijke interbestuurlijke stuurgroep/adviesraad.

## Met instemmen op de resolutie dragen de leden van de VNG het bestuur van de VNG op om bij het Rijk en ketenpartners het volgende te bewerkstelligen:

***1. De BIG als basisnormenkader voor het gemeentelijke domein wordt erkend.***

De BIG wordt middels deze resolutie door de gemeenten benoemd als het geldende normenkader voor alle gemeenten. Gemeenten verwachten hierbij dat de (bestuurlijke) (keten)partners, en eventueel het College Standaardisatie, de BIG eveneens erkennen als normenkader voor het gemeentelijk domein. Dit houdt in dat het Rijk volgens het 'pas toe of leg uit' principe naar de BIG verwijst wanneer informatieveiligheid bij gemeenten in het spel is. Bij nieuwe wet- en regelgeving die een relatie heeft met de informatieveiligheid bij gemeenten zal het Rijk uitleg moeten geven wanneer er meer, of andere normen gebruikt worden dan opgenomen in de BIG.

Gemeenten moeten erop kunnen vertrouwen dat de partners dit uitgangspunt (blijven) hanteren. De VNG wordt hiervoor door de BALV gevraagd om deze interbestuurlijke erkenning te borgen door dit ter instemming in te brengen in het bestuurlijk overleg met minister Plasterk van BZK.
Zoals nu al gebruikelijk, wordt bij nieuwe wet- en regelgeving een bestuurlijke en een informatiekundige uitvoeringstoets gedaan. Als vast onderdeel van de informatiekundige uitvoeringstoets zal daarom in het vervolg moeten worden getoetst op het hanteren van het 'pas toe of leg uit principe' in relatie tot de BIG.

***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.***

De auditlast voor gemeenten is hoog, denk bijvoorbeeld aan de opgelegde auditverplichtingen voor SUWI, het GBA, de BAG en het gebruik van DigiD. Deze last drukt zich uit in een aanzienlijke personele inspanning en financiële druk per audit . In de praktijk blijkt daarnaast dat er een overlap bestaat tussen deze verschillende auditverplichtingen.

Gemeenten maken, vanuit de eigen verantwoordelijkheid, werk van informatieveiligheid zoals geschetst in deze resolutie. Willen gemeenten zowel organisatorisch als financieel in staat zijn/blijven om informatieveiligheid adequaat te adresseren, dan moet de auditverplichting voor gemeenten worden verlaagd. Dit past in het kader van zelfregulering op informatieveiligheid dat uitgaat van horizontaal toezicht en horizontale sturing.

Gemeenten vragen daarom regie op rijksniveau om te werken aan beperking van de audit- en monitoringlast, en mogelijk op termijn afschaffen van audits. Een eenduidige regieorganisatie, bij voorkeur het ministerie van BZK met de minister als verantwoordelijke, die expliciet verantwoordelijkheid neemt voor het beperken van de audit- en monitoringlast is van essentieel belang om hier resultaten te halen. Hiernaast moeten duidelijke afspraken komen over de verschillende verantwoordelijkheden van centrale voorzieningen zoals Logius en NCSC in relatie tot gemeenten. Dit vereist departementale coördinatie waarvoor het ministerie van BZK de meest aangewezen partij is.

Gemeenten vragen hierbij gebruik te maken van hetgeen al beschikbaar is en verwijzen (keten)partners naar waarstaatjegemeente.nl. Informatie die hierop wordt gedeeld is openbaar en geaccordeerd door de lokale volksvertegenwoordiging en dient derhalve voldoende inzicht te geven aan (keten) partners.

*3. Gemeenten voldoende tijd krijgen voor een gefaseerde en gedifferentieerde implementatie van informatieveiligheid die gebaseerd is op lokale afwegingen en financieringsmogelijkheden.*

Waar de ene gemeente informatieveiligheid professioneel heeft georganiseerd, kan de andere zich hier nog op ontwikkelen. Het vergt tijd om informatieveiligheid bij alle gemeenten op een zelfde niveau te brengen.

Gemeenten beseffen zich terdege dat het volledig implementeren van alle mogelijke maatregelen geen sinecure is. De complexiteit en omvang van informatieveiligheid leent zich derhalve voor een gefaseerde implementatie. Gemeenten hebben, kortom, tijd nodig voor een realistische implementatie. Burgers, bedrijven en (keten)partners mogen tegelijk ook van gemeenten verwachten dat eventueel bestaande risico's zo spoedig mogelijk moeten worden gemitigeerd.

Omdat de ene gemeente de andere niet is, zetten gemeenten in op een lokale implementatie van de normen. Lokaal voert de gemeente hiervoor een nulmeting uit, waarna op basis van (bestuurlijke) risico-afwegingen en door de gemeenteraad gestelde (financiële) kaders speerpunten worden benoemd en aangepakt.

VNG en IBD (KING) adviseren gemeenten hierbij om in ieder geval werk te maken van de processen rondom de GBA en de BGT. Ook in het kader van de drie decentralisaties zal de gemeente verantwoordelijkheid moeten nemen op informatieveiligheid. Daarnaast adviseert de VNG gemeenten om organisatorische aansluiting te realiseren bij de IBD. Hiermee wordt de gemeente snel geïnformeerd en geadviseerd bij eventuele acute en/of kritische veiligheidslekken in een van de gemeentelijke systemen.

*4. Helderheid komt over een voor gemeenten werkbare meldplicht bij datalekken.*

Het Rijk bereidt wetgeving voor omtrent het melden van datalekken en technische incidenten. Deze wetgeving heeft impact op gemeenten. Het moet voor gemeenten duidelijk zijn of, en onder welke voorwaarden, hierover gemeld moeten worden. Ook moet duidelijk zijn bij welke instanties gemeld kan worden. Hierbij moet uitgezocht worden of en welke rol de IBD kan innemen bij de coördinatie van verplichte meldingen en op welke manier deze rol moet worden gefinancieerd.

*5. Een externe adviserende (interbestuurlijke) visitatiecommissie, gefinancierd door het Rijk.*

Gemeenten stellen voor gebruik te maken van de opgedane kennis en methodiek van zelfleren, zelfreguleren, monitoren en toezicht bij dossier riolering en waterzuivering. Gemeenten, waterschappen, provincies en Rijk hebben op dit dossier goede ervaringen opgedaan met een omvangrijke en complexe implementatie van zelfregulering, monitoring en verantwoording. Uit deze ervaringen blijkt dat een gefaseerde implementatie van regulering door middel van een interventieladder een goede methode is voor het verhogen van kwaliteit.

Gemeenten roepen de interbestuurlijke partners op om in gezamenlijkheid deze systematiek voor zelfregulering toe te passen voor informatieveiligheid.

Belangrijk onderdeel van deze systematiek is een onafhankelijke, bij voorkeur, interbestuurlijke visitatiecommissie die een adviserende rol richting gemeenten inneemt. Deze visitatiecommissie krijgt het doel om het leren bij gemeenten te stimuleren. Hiernaast kan de visitatiecommissie toetsen in hoeverre het systeem van zelfregulering werkt. Voor dit tweede doel zal de visitatiecommissie rapporteren (op geaggregeerd niveau) aan een, nog in te stellen, hoog ambtelijke interbestuurlijke stuurgroep waarin onder andere de VNG zitting krijgt.

Gemeenten vragen het ministerie van BZK als stelselverantwoordelijke om de visitatiecommissie te

financieren. Dit is nodig om de onafhankelijkheid ervan te garanderen. Bovendien heeft de stelselverantwoordelijke ook de verantwoordelijkheid om inzicht te krijgen in de werking van zelfregulering over de verschillende overheidslagen heen.

***6. Wet- en regelgeving zo beperkt mogelijk wordt gehouden.***

Wetgeving is een mogelijk middel om een basis te bieden voor de zelfregulering op informatieveiligheid, zoals deze door gemeenten binnen deze resolutie is uitgewerkt. Hiertoe vragen gemeenten de VNG om hierover met het Rijk een verkenning te doen.

Onderzocht moet worden of er (kleine) aanpassingen nodig zijn in wet- of regelgeving om het systeem van zelfregulering op informatieveiligheid te doen slagen. Gedacht wordt in ieder geval om uit te zoeken of opname van informatieveiligheid in het gemeentelijk jaarverslag in regelgeving moet worden verankerd. Om regeldruk te minimaliseren moet anderzijds verkend worden welke bestaande wetgeving overbodig is of op termijn kan worden.

## En dragen de VNG op om:

1. ***De doorontwikkeling van de BIG organisatorisch te borgen.***

Omdat de omgeving waarbinnen gemeenten bewegen continue in verandering is, is de BIG geen statisch document: het beweegt met de omgeving mee. De BALV mandateert het VNG-bestuur daarom tot beheer van de BIG. Het VNG-bestuur zal hierbij nadrukkelijk steunen op de expertise van KING/IBD en aansluiting zoeken over de verschillende overheidsdomeinen heen.

2. ***Samen met het Rijk, ketenpartners en KING te verkennen hoe leveranciers beter kunnen worden betrokken bij het borgen van informatieveiligheid.***

VNG wil met het Rijk, ketenpartners en KING verkennen op welke manier bij leveranciers een zelfde gevoel van urgentie bereikt kan worden om informatieveiligheid prominent op de agenda te krijgen – en te houden.

3. ***Individuele gemeenten blijven aansporen tot het instellen van lokaal informatieveiligheidsbeleid.***

Alle gemeenten zijn afhankelijk van elkaar. Mede omdat het beeld over alle gemeenten voor een groot deel beïnvloed kan worden door hoe individuele gemeenten in het nieuws komen. Vanwege deze afhankelijkheid spoort de VNG alle gemeenten aan om informatieveiligheid op orde te hebben.