Vereniging van
Nederlandse Gemeenten

Brief aan de leden
T.a.v. het college en de raad

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8393		-
betreft	**ons kenmerk**	**datum**
Informatieveiligheid en privacy	ECIB/U201700133 Lbr. 17/010	20 februari 2017

Samenvatting

Het grootste deel van de gemeentelijke dienstverlening verloopt inmiddels digitaal. Uw verantwoordelijkheid voor een zorgvuldige omgang met informatie is daarmee net zo vanzelfsprekend als uw verantwoordelijkheid voor mensen, middelen en financiën.

Informatieveiligheid en privacy zijn thema's die hierbij doorlopend aandacht verdienen. Informatieveiligheid gaat om beschikbaarheid, vertrouwelijkheid en integriteit. Samengevat: werkt het? Kan er niemand bij de informatie die daar niet bij mag? Zijn de gegevens juist en volledig? Privacy gaat over de zorgvuldige omgang met persoonlijke gegevens en de bescherming van de persoonlijke levenssfeer van uw inwoners.

Een groot misverstand is dat informatieveiligheid en privacy vooral te maken hebben met techniek en ICT. De veilige omgang met informatie heeft te maken met de organisatie, de werkprocessen, beschermingsmaatregelen en de controle op alledrie.

Er is in de afgelopen tijd veel aandacht voor hacks, onveilige websites en datalekken bij gemeenten.

De VNG raadt aan om regelmatig contact te hebben met uw functionaris informatiebeveiliging (CISO) en actief aandacht te hebben voor maatregelen om de bedreigingen tegen te gaan.

Wij informeren u in deze brief over de belangrijkste ontwikkelingen op dit onderwerp. Achtereenvolgens gaat het over de manier waarop u verantwoording aflegt over informatieveiligheid richting de gemeenteraad en de rijksoverheid, de ondersteuning van de Informatiebeveiligingsdienst (IBD), de invoering van de nieuwe Europese Privacyrichtlijn en het ondersteuningsaanbod van de VNG en KING.

Vereniging van
Nederlandse Gemeenten

Aan de leden

informatiecentrum tel.	uw kenmerk	bijlage(n)
(070) 373 8393		-
betreft	**ons kenmerk**	**datum**
Informatieveiligheid en privacy	ECIB/U201700133 Lbr. 17/010	20 februari 2017

Geacht college en gemeenteraad,

Het grootste deel van de gemeentelijke dienstverlening verloopt inmiddels digitaal. Uw verantwoordelijkheid voor een zorgvuldige omgang met informatie is daarmee net zo vanzelfsprekend als uw verantwoordelijkheid voor mensen, middelen en financiën.

Informatieveiligheid en privacy zijn thema's die hierbij doorlopend aandacht verdienen. Informatieveiligheid gaat om beschikbaarheid, vertrouwelijkheid en integriteit. Samengevat: werkt het? Kan er niemand bij de informatie die daar niet bij mag? Zijn de gegevens juist en volledig? Privacy gaat over de zorgvuldige omgang met persoonlijke gegevens en de bescherming van de persoonlijke levenssfeer van uw inwoners.

Een groot misverstand is dat informatieveiligheid en privacy vooral te maken hebben met techniek en ICT. De veilige omgang met informatie heeft te maken met de organisatie, de werkprocessen, beschermingsmaatregelen en de controle op alledrie.

Er is in de afgelopen tijd veel aandacht voor hacks, onveilige websites en datalekken bij gemeenten. De belangrijkste bedreigingen voor gemeenten zijn:

- onvoldoende naleving van de normen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- onvoldoende zicht op incidenten in uw ICT-landschap, gebrek aan detectie
- onzorgvuldig werken, bijvoorbeeld door verkeerd geadresseerde brieven en e-mails
- misbruik van kwetsbaarheden in uw organisatie, bijvoorbeeld door phishing e-mails en virussen
- onvoldoende aandacht voor veiligheid en privacy, bijvoorbeeld bij de uitvoering van het werk en afspraken met toeleveranciers
- imagoschade door incidenten bij uw organisatie, andere gemeenten en (mede)overheden

Die bedreigingen brengen risico's met zich ten aanzien van de betrouwbaarheid van de informatie. Een betrouwbare informatievoorziening is belangrijk voor de lokale democratie, aangezien de gemeenteraad en het college besluiten nemen op basis van deze informatie. Informatie dient beschikbaar, juist, tijdig en actueel te zijn, waarbij informatie niet geraadpleegd mag worden door onbevoegden. Belangrijk is daarbij dat de persoonsgegevens adequaat

worden beveiligd om de privacy van uw inwoners te beschermen en bijvoorbeeld identiteitsfraude te voorkomen.

De VNG raadt aan om regelmatig contact te hebben met uw functionaris informatiebeveiliging (CISO) en actief aandacht te hebben voor maatregelen om de bedreigingen tegen te gaan en risico's te beheersen: bijvoorbeeld door te werken aan bewustwording, en het implementeren van juiste en werkbare beveiligingsmaatregelen (organisatie, processen en techniek).

Wij informeren u in deze brief over de belangrijkste ontwikkelingen op dit onderwerp. Achtereenvolgens gaat het over de manier waarop u verantwoording aflegt over informatieveiligheid richting de gemeenteraad en de rijksoverheid, de ondersteuning van de Informatiebeveiligingsdienst (IBD), de invoering van de nieuwe Europese Privacyrichtlijn en het ondersteuningsaanbod van de VNG en KING.

Verantwoording Informatieveiligheid, ENSIA
Gemeenten leggen verantwoordelijkheid af over hun informatieveiligheid in het jaarverslag, dit is in 2013 afgesproken in de resolutie 'informatieveiligheid, randvoorwaarde voor de professionele gemeente'.

In 2017 gebeurt dit voor het eerst met een nieuwe Audit systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). Deze nieuwe systematiek maakt het inzicht in de stand van zaken rondom informatieveiligheid gemakkelijker en efficiënter. Met ENSIA wordt de situatie van de gemeente getoetst aan de normen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Met ENSIA sluit de horizontale verantwoording over informatieveiligheid aan op de planning en control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad.

ENSIA structureert ook de verticale verantwoording richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

Binnenkort verschijnt een ledenbrief ENSIA waarin u nader wordt geïnformeerd over de stappen die uw gemeente moet nemen om een en ander te realiseren.

Verhoogde aandacht Informatiebeveiligingsdienst (IBD) voor detectie en preventie van incidenten
De Informatiebeveiligingsdienst (IBD) ondersteunt ook uw gemeente op het gebied van informatiebeveiliging. De IBD staat 24x7 klaar voor gemeenten in het geval van een informatiebeveiligingsincident zoals een datalek. Naast incidentondersteuning biedt de IBD ook advies, over beleid, maar ook over bijvoorbeeld woordvoering en communicatie.
De IBD informeert gemeenten op maat over incidenten in hun ICT-landschap. Daartoe is het wel van belang dat gemeenten aangeven over welke specifieke systemen en producten ze waarschuwingen willen ontvangen. Nog niet iedere gemeente heeft dit gedaan.

De IBD zal in 2017 verhoogde prioriteit geven aan de detectie en mogelijke preventie van incidenten bij gemeenten. De IBD voert een verkenning uit naar de mogelijkheden om dreigingsinformatie (Threat Intelligence) te verzamelen, veredelen, verrijken en te delen met en tussen gemeenten. Doordat gemeenten onderling dreigingsinformatie met elkaar delen, maken gemeenten elkaar sterker. Detectie van een dreiging bij de ene gemeente, leidt hiermee tot

preventie van diezelfde dreiging bij de andere gemeenten. Dit is nodig om nieuwe risico's en dreigingen het hoofd te kunnen bieden. De IBD verkent in 2017 de behoefte van de doelgroep aan nieuwe producten en diensten op dit vlak.

De VNG roept op om het aansluitproces bij de IBD te voltooien indien dit nog niet is gedaan.

Aansluiten samenwerkingsverbanden IBD
De verantwoordelijkheid van het gemeentebestuur voor informatiebeveiliging is niet beperkt tot de eigen organisatie, deze geldt ook in gemeenschappelijke regelingen of samenwerkingsverbanden.

Op verzoek van de adviesraad van de IBD waarin gemeenten bestuurlijk vertegenwoordigd zijn, is in 2016 een verkenning uitgevoerd naar de mogelijkheden om samenwerkingsverbanden ook aan te sluiten bij de IBD. Op basis van de uitkomsten van de verkenning kunnen intergemeentelijke sociale diensten en belastingsamenwerkingen vanaf januari 2017 aansluiten. De dienstverlening aan deze samenwerkingen past binnen de huidige financiële kaders. Er zijn derhalve geen additionele kosten voor gemeenten of hun samenwerkingsverbanden aan verbonden.

Wij verzoeken u deze informatie door te geleiden naar het dagelijks bestuur van uw eventuele intergemeentelijke sociale dienst ofwel uw belastingsamenwerking. Voor meer informatie kunt u contact opnemen met de IBD via 070 373 8011 of info@IBDgemeenten.nl.

Privacy – Nieuwe Europese privacywetgeving vraagt om nieuw denken én handelen
Het Europese Parlement en de Raad hebben op 27 april 2016 officieel ingestemd met de Algemene Verordening Gegevensbescherming. De definitieve tekst is daarna op 4 mei 2016 gepubliceerd in het publicatieblad van de Europese Unie (Pb EU L119), waarna de verordening op 25 mei 2016 in werking is getreden. De Verordening heeft een directe werking en hoeft niet meer in nationale wetgeving geïmplementeerd te worden. Alle organisaties in de publieke en private sector hebben nu tot 25 mei 2018 om volledig aan de nieuwe wetgeving te voldoen. [1] De AVG brengt met zich mee dat gemeenten verplicht zijn om een functionaris gegevensbescherming aan te stellen.

Met de invoering van de AVG verscherpen de eisen waaraan verwerkingen van persoonsgegevens moeten voldoen. De AVG vraagt echter om meer dan enkel ordentelijk met persoonsgegevens omgaan: de AVG vraagt om nieuw denken én handelen. Zo hebben uw inwoners het recht op inzage in waar u welke gegevens van ze verwerkt. Inwoners hebben straks ook het recht om 'vergeten' te worden. Dat wil zeggen dat ze het recht hebben om zich te laten verwijderen uit databases, tenzij legitieme wettelijke vereisten dit voorkomen. Het in kaart hebben van de wettelijke grondslag van verwerking van persoonsgegevens is in dit kader van groot belang.

Dankzij deze nieuwe wetgeving dringt gegevensbescherming en privacy door in alle processen binnen de gemeentelijke organisatie. De VNG adviseert om op korte termijn een functionaris gegevensbescherming aan te stellen die de implementatie kan coördineren.

De VNG en KING werken in 2017 aan een integraal ondersteuningsaanbod op het thema privacy. VNG en KING ontwikkelen een set aan handreikingen en factsheets in nauwe afstemming met gemeenten, de IBD en privacy experts. Hierbij zullen waar mogelijk initiatieven van mede-overheden worden meegenomen, zoals de handreikingen en het privacy-raamwerk van het Centrum voor Informatiebeveiliging en Privacy van Belastingdienst, DUO, SVB en UWV.

[1] voor meer informatie over de AVG, zie de ledenbrief van 12 juli 2016: https://vng.nl/files/vng/brieven/2016/20160712_ledenbrief_algemene-verordening-gegevensbescherming.pdf).

Hoogachtend,

Vereniging van Nederlandse Gemeenten

J. Kriens
Algemeen Directeur

Deze ledenbrief staat ook op www.vng.nl onder brieven.