Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1327

Vragen van het lid **Oosenbrug** (PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *de berichten «Datalekken bij gemeenten; het is een beetje een zooitje» en «Organisaties worstelen met nieuwe privacy wetgeving»* (ingezonden 2 februari 2017).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 1 maart 2017)

Vraag 1
Kent u de berichten «Datalekken bij gemeenten; «het is een beetje een zooitje»» en «Organisaties worstelen met nieuwe privacy wetgeving»?[1] [2]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat het schokkend is dat het beleid rond datalekken bij gemeenten nog steeds een zooitje is, dat gemeenten geen eenduidig beleid voeren rond datalekken, en dat datalekken niet altijd gemeld worden bij de Autoriteit Persoonsgegevens, terwijl dit wel verplicht is sinds januari 2016? Zo ja, hoe is het dan mogelijk dat gemeenten zich nog steeds in heel verschillende mate bewust zijn van de datalekken in hun organisatie en dat nog steeds niet binnen alle gemeenten bekend is dat bijvoorbeeld een verloren usb-stick met gevoelige gegevens ook een datalek is? Zo nee, waarom niet?

Antwoord 2
Ik deel het geschetste beeld niet. Niet ieder beveiligingsincident is een datalek en niet ieder datalek is meldplichtig. Gemeenten zijn gehouden aan de meldplicht datalekken en de beleidsregels die de Autoriteit Persoonsgegevens (AP) heeft opgesteld, die organisaties helpen bij het bepalen of er sprake is van een datalek. Het is aan AP om te bepalen of organisaties daarin in gebreke zijn.

---

[1] https://www.nrc.nl/nieuws/2017/01/27/datalekken-bij-gemeenten-het-is-een-beetje-een-zooitje-6438132-a1543413

[2] http://www.binnenlandsbestuur.nl/digitaal/nieuws/organisaties-worstelen-met-nieuwe.9557231.lynkx

ah-tk-20162017-1327
ISSN 0921 - 7398
's-Gravenhage 2017

Gemeenten worden bij hun informatiebeveiliging ondersteund door de Informatiebeveiligingsdienst (IBD). De IBD heeft ondersteuningsproducten ontwikkeld en beschikbaar gesteld aan gemeenten. Daarnaast biedt de helpdesk van de IBD hulp bij de beoordeling van de vraag of een beveiligingsincident een datalek is en of gemeld moet worden bij de AP en/of betrokkenen.
De AP heeft aangekondigd om de gemeenten via de VNG nogmaals te wijzen op welke lekken wel en welke lekken niet gemeld dienen te worden.
Het college van burgemeester en wethouders is verantwoordelijk voor informatiebeveiliging in de eigen organisatie. Ik wijs erop dat gemeenten ook collectief hun verantwoordelijkheid nemen. De gemeenten hebben zich tijdens de bijzondere ALV van de VNG van 2013 via de resolutie «Informatieveiligheid, randvoorwaarde voor de professionele gemeente» gecommitteerd aan de baseline informatiebeveiliging gemeenten (BIG). Dat gezamenlijk normenkader biedt voldoende handvatten om een solide informatieveiligheidsbeleid te voeren. Het is aan de gemeenteraad om het college hierop te controleren. Los van het beleid zijn gemeenten natuurlijk gehouden aan de wettelijke kaders en verplicht om zorgvuldig om te gaan met gegevens.

Vraag 3
Deelt u de mening dat het tevens zeer schokkend is dat slechts bij 18% van de datalekken bij gemeenten dit aan de betrokkenen gemeld is? Deelt u de mening dat betrokkenen altijd op de hoogte moeten worden gesteld van een datalek aangezien hun gegevens kunnen worden misbruikt? Zo ja, hoe gaat u gemeenten hierop aanspreken? Zo nee, waarom niet?

Antwoord 3
Als een lek aan de Autoriteit Persoonsgegevens moet worden gemeld, betekent dat niet automatisch dat dit ook aan de betrokkene dient te worden gemeld. De gemeente waar het lek zich voordoet moet daarvoor een aparte afweging maken. De Wet bescherming persoonsgegevens (Wbp) geeft aan dat een melding gedaan moet worden aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Het is niet aan mij om de genoemde gevallen te beoordelen of het melden of niet melden aan betrokkenen rechtmatig is; dat is aan de toezichthouder, de AP.

Vraag 4
Hoe is het mogelijk dat de Autoriteit Persoonsgegevens op dit moment nog geen boetes heeft uitgedeeld aan gemeenten die hun informatiebeveiliging niet op orde hebben? Deelt u de mening dat het huidige beleid rond informatiebeveiliging te vrijblijvend is en gemeenten harder aangepakt moeten worden om hen te motiveren aan hun verplichtingen met betrekking tot het beschermen van privacy en persoonsgegevens te voldoen? Zo ja, wat gaat u hieraan doen? Zo, nee waarom niet?

Antwoord 4
Informatiebeveiliging bij gemeenten is niet vrijblijvend. Informatiebeveiliging is krachtens de Wbp verplicht. De wetgever heeft de Autoriteit Persoonsgegevens ingesteld om toezicht op de naleving van de wet uit te oefenen. De AP is onafhankelijk. Het is daarom aan de AP en niet aan mij om te besluiten of een boete of een andere interventie op zijn plaats is.
Informatiebeveiliging is een verantwoordelijkheid van de gemeente zelf, waarbij de gemeenteraad een controlerende taak heeft. Ik moet die positie van de gemeenten respecteren en onthoud mij daarom van een oordeel ter zake. De AP heeft, zoals ik aangeef in het antwoord op vraag 2, aangekondigd om de gemeenten nogmaals te wijzen op welke lekken wel en welke lekken niet gemeld dienen te worden.

Vraag 5
Hoe beoordeelt u de onderzoeken van Reporter-radio (KRO-NCRV) en PwC waaruit blijkt dat gemeenten blijkbaar toch niet zelf in staat zijn om de door hun gebruikte informatiesystemen te beveiligen? Hoe beziet u dit in het licht

van uw antwoorden op eerdere vragen over datalekken bij gemeenten[3] waarin u stelt dat dit een verantwoordelijkheid van gemeenten zelf is?

Antwoord 5
Zoals ik in de beantwoording van vraag 4 aangeef, is de beveiliging van informatie een verantwoordelijkheid van de gemeente zelf. Dat er zich incidenten voordoen, betekent mijns inziens niet dat gemeenten niet in staat zijn zelf hun informatiesystemen te beveiligen. Gemeenten worden daarbij actief door de VNG, in het bijzonder de IBD, ondersteund. Daarnaast is het belangrijk dat AP haar werk doet.

Vraag 6
Deelt u de zorgen van de indiener over de uitkomst van het PwC Privacy Governance onderzoek dat slechts een op de tien organisaties klaar is voor de gewijzigde privacywetgeving die in mei 2018 van kracht wordt?

Antwoord 6
In het Privacy governance onderzoek onder 210 organisaties in onder meer de publieke sector geeft 9% van de organisaties aan nu al te voldoen aan de verplichting uit de Algemene Verordening Gegevensbescherming (AVG) om alle verwerkingen van persoonsgegevens inzichtelijk te hebben en te documenteren. Dat is voor deze organisaties een belangrijke stap in de goede richting, maar – zonder de specifieke situatie per organisatie te kennen – zullen ook deze organisaties waarschijnlijk nog verdere stappen moeten ondernemen om aan de AVG te voldoen. Ook hiervoor geldt dat elke organisatie, publiek en privaat, zelf verantwoordelijk is voor naleving van de regels in de AVG en de daarop gebaseerde wetgeving. Dit is inherent aan het juridische systeem van de AVG die elke verantwoordelijke voor gegevensverwerking zelf de verantwoordelijkheid oplegt voor naleving ervan. Vanuit de departementen en koepelorganisaties worden wel enkele faciliterende activiteiten ondernomen om organisaties te ondersteunen bij de implementatie.

Vraag 7
Hoe beoordeelt u het resultaat van het onderzoek van PwC dat het erop lijkt dat nog weinig organisaties de voorbereiding op de Algemene Verordening Gegevensbescherming (AVG) in gang hebben gezet en dat slechts 22 procent van de organisaties met regelmaat risicoanalyses zoals het privacy impact assessment uitvoert?

Antwoord 7
Uit het onderzoek blijkt dat 55% van de onderzochte organisaties standaard of ad-hoc privacy impact assessments uitvoert. 39% doet dit niet en 6% van de respondenten geeft aan het niet te weten.
Sinds 1 september 2013 wordt de PIA standaard toegepast bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien (Kamerstuk 26 643 nr. 282).
De beroepsorganisatie van IT-auditors (NOREA) heeft een handreiking voor de uitvoering van een PIA ontwikkeld die breed wordt gebruikt. Ook diverse sectoren, bijvoorbeeld de onderwijssector die werkt met een model PIA van de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland (SURF), zijn hier voortvarend mee aan de slag. Het is een goed teken dat organisaties, zowel bij overheid als bedrijfsleven, nu al aan de slag zijn zonder dat er een wettelijke verplichting geldt.

Vraag 8
Hoe beoordeelt u dit resultaat in het licht van uw antwoorden op mijn eerdere vragen[4] waarin u stelt dat organisaties zelf verantwoordelijk zijn voor het beveiligen van de door hen gebruikte informatiesystemen? Deelt u de mening dat uit de onderzoeken blijkt dat gemeenten op dit punt onvoldoende hun verantwoordelijkheid nemen? Zo ja, wat gaat u hieraan doen? Zo nee,

---

[3] Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 813
[4] Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 813

wat is volgens u de reden dat gemeenten de voorbereidingen op de AVG nog niet in gang hebben gezet en wat gaat u doen om dit probleem aan te pakken?

Antwoord 8
Ik kan op basis van de onderzoeken geen conclusies trekken over hoe ver de gemeenten zijn met het zich voorbereiden op de AVG. Ook voor de implementatie zijn de gemeenten zelf verantwoordelijk. De IBD helpt de gemeenten bij de implementatie en heeft daarvoor een aantal specifieke middelen ontwikkeld.

Vraag 9
Deelt u de mening dat het onacceptabel is dat slechts 31% van de deelnemers aan het PwC Privacy Governance onderzoek bij de ontwikkeling en implementatie van nieuwe systemen rekening houdt met de verplichting om aandacht te hebben voor privacy van betrokkenen en de bescherming van persoonsgegevens?

Antwoord 9
Gevraagd naar de stelling «Bij implementatie van nieuwe systemen houden wij altijd in een vroeg stadium rekening met privacy aspecten en de bescherming van persoonsgegevens (Privacy by Design principe)» gaf 31% van de respondenten aan daar nu al rekening mee te houden en 69% niet. In het huidige wettelijke kader van de Wbp is er nog geen wettelijke verplichting om het Privacy by Design principe toe te passen, hoewel dit wel wenselijk is. Onder de AVG wordt de verwerkingsverantwoordelijke verplicht zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen (*privacy by design* en *privacy by default*). In dat licht beoordeel ik dat 31% van de respondenten nu al voldoet, zonder dat er een wettelijke plicht is, als positief.

Vraag 10
Bent u het ermee eens dat dit zeer zorgelijk is en ertoe leidt dat het probleem met datalekken in stand blijft en datalekken aan de orde van de dag blijven?

Antwoord 10
Net als de Autoriteit Persoonsgegevens ben ik van mening dat PIA's en de principes van Privacy by Design, waaronder dataminimalisatie, een positieve bijdrage kunnen leveren aan het voorkomen van datalekken en daarmee aan de bescherming van persoonsgegevens. Dat is ook precies de reden dat deze principes, die bijvoorbeeld door het Rijk zijn omarmd, een plaats hebben gekregen in de AVG. Dat neemt niet weg dat de zorg voor een afdoende niveau van beveiliging van persoonsgegevens een blijvende verplichting is.

Vraag 11
Gaat u alle gemeenten verplichten zich te verantwoorden over de kwaliteit van hun informatieveiligheid met ENSIA per 1 juli 2017? Verwacht u dat datalekken hierdoor sterk zullen verminderen? Zo ja, waarom?

Antwoord 11
Het project ENSIA heef tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de BIG.
ENSIA gaat gemeenten helpen om meer inzicht te krijgen in de stand van zaken van de informatieveiligheid zodat ze er beter op kunnen sturen. ENSIA betreft een methodiek die een aantal reeds bestaande assessments/audits op het zelfde moment uitvraagt, waarbij door middel van een collegeverklaring informatiebeveiliging, een assurancerapport door een IT-auditor en een paragraaf informatiebeveiliging in het jaarverslag verantwoording wordt afgelegd aan de raad en aan de betrokken departementen.
Als ENSIA per 1 juli 2017 wordt ingevoerd dan gaan de gemeenten zich in 2018 over 2017 verantwoorden – in eerste instantie aan hun eigen gemeenteraad en in tweede instantie aan de desbetreffende departementen (BZK,SZW en I&M).

Datalekken zijn overigens niet alleen afhankelijk van de beveiliging van ICT-systemen, maar kunnen ook te maken hebben met het menselijk handelen, denk bijvoorbeeld aan het verliezen van een USB-stick met privacygevoelige informatie. Door invoering van ENSIA wordt wel verwacht dat in ieder geval het bewustzijn rondom informatieveiligheid bij gemeenten zal toenemen.

Vraag 12
Deelt u de mening dat 1 juli 2017 te laat is om dit probleem aan te pakken aangezien datalekken aan de orde van de dag zijn en er een risico bestaat dat er veel gevoelige informatie op straat komt te liggen of misbruikt kan worden?

Antwoord 12
De datum van 1 juli is gekozen als realistische datum waarop alle betrokken organisaties verwachten klaar te zijn voor de invoering van deze nieuwe wijze van verantwoorden. Versnelde invoering is niet mogelijk doordat de gemeenten hiervoor klaar moeten zijn, het instrument ook ontwikkeld dient te zijn en de afspraken met de IT-auditors gemaakt moeten zijn.

Vraag 13
Kunt u garanderen dat na de implementatie van ENSIA informatieveiligheid niet onderworpen wordt aan een eenmalige of ad hoc kwaliteitsmeting maar dat gemeenten vaker verantwoording dienen af te leggen waardoor de informatie continue beveiligd blijft?

Antwoord 13
ENSIA is niet eenmalig of ad hoc. De ENSIA-verantwoording sluit aan op de jaarlijkse planning- en controlecyclus van de gemeenten. Bovendien hebben de gemeenten met elkaar afgesproken dat zij zich jaarlijks willen verantwoorden via een aparte paragraaf over informatiebeveiliging over de volle breedte van de BIG in het gemeentelijk jaarverslag. Voorts dient via ENSIA jaarlijks verantwoording te worden afgelegd aan de departementen (aan BZK over DigiD, BRP en PUN, aan SZW over SUWInet en I&M over BAG/BGT).

Vraag 14
Bent u het ermee eens dat, om dit probleem aan te pakken en de informatiebeveiliging bij gemeenten structureel te verbeteren, gemeenten een autonoom budget moeten krijgen om informatieveiligheid op peil te houden en dat dit budget niet gekoppeld moet worden aan individuele systemen?

Antwoord 14
Ik ben van mening dat besluitvorming over het gewenste niveau van informatieveiligheid bij gemeenten en over de eventuele noodzaak tot prioritering daarin het beste op lokaal niveau kan plaatsvinden. Ik acht het op voorhand niet noodzakelijk om budgetten voor gemeenten af te zonderen of te oormerken. Een dergelijke maatregel verplicht gemeenten om een ontvangen budget voor informatieveiligheid aan dat doel te besteden. Informatieveiligheid behoeft een integrale inbedding in de organisatie – een benadering die verder strekt dan ICT. Het gaat om organisatie, processen, fysieke maatregelen en ICT.

Vraag 15
Hoe garandeert u dat binnen gemeenten aanbestede informatiesystemen ook na oplevering worden bijgewerkt? Is dit ook onderdeel van de Gemeentelijke inkoopvoorwaarden bij IT? Zo nee, waarom niet? Deelt u de mening dat dit een minimale eis bij het aanbestedingsproces zou moeten zijn?

Antwoord 15
De Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) zijn donderdag 8 december 2016 vastgesteld door het Verenigingsbestuur van de VNG. De totstandkoming van de GIBIT is onderdeel van het programma Digitale Agenda 2020 die als één van de speerpunten heeft om het ICT-opdrachtgeverschap bij gemeenten te professionaliseren.
Voor de kwaliteit van hun dienstverlening en uitvoering zijn gemeenten steeds meer afhankelijk van ingekochte ICT-producten en -diensten. Deze

producten en diensten worden geleverd door bijna tweehonderd verschillende leveranciers. Gemeentelijke Inkoopvoorwaarden helpen gemeenten om te waarborgen dat ze een product krijgen dat ze echt willen, waarvoor duidelijke afspraken zijn gemaakt en dat aansluit bij hun behoefte en doelstellingen. Gemeenten en gemeentelijke samenwerkingsverbanden wordt aanbevolen de GIBIT op te nemen in het inkoopbeleid en te gebruiken bij de inkoop van IT.
In de GIBIT zijn specifieke artikelen opgenomen over privacy, beveiliging en archivering. Het hoofdstuk is van toepassing zodra er (persoons)gegevens met de ICT Prestatie worden verwerkt. Dat zal heel vaak het geval zijn, maar zeker niet altijd (bijv. niet bij hardware).
De GIBIT stelt gemeenten nadrukkelijk in staat om met informatiesystemen te kunnen voldoen aan de Baseline Informatie Beveiliging (BIG). Dit wordt onder meer gedaan via de Gemeentelijke ICT-kwaliteitsnormen waarin de BIG is verankerd. In de GIBIT zijn voorzieningen opgenomen dat leveranciers blijvend moeten voldoen aan deze Gemeentelijke ICT-kwaliteitsnormen, ook indien die normen aangepast worden. Hiermee wordt beoogd dat ook na oplevering bestaande informatiesystemen worden bijgewerkt. Gezien dat deze normen via de GIBIT worden geborgd wordt gemeenten aangeraden om de GIBIT inclusief deze bepalingen van toepassing te verklaren.
In de BIG is het de norm dat tijdig informatie dient te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen (lees: updates en patches) voor behandeling van daarmee samenhangende risico's.