



Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

> Retouradres

Turfmarkt 147  
Den Haag  
Postbus 20011  
2500 EA Den Haag  
[www.rijksoverheid.nl](http://www.rijksoverheid.nl)

**Kenmerk**  
2013-0000762191

**Uw kenmerk**  
DC2013/03/b

**Bijlagen**  
2

**Datum** 18 december 2013  
**Betreft** Beslissing op uw Wob-verzoek

Bij brief van 9 september 2013, door mij ontvangen op 11 september 2013, heeft u bij mijn ministerie een verzoek ingediend als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (hierna: Wob). Uw verzoek heeft betrekking op de Patriot Act.

U vraagt om openbaarmaking van

- "1. (Externe) adviezen, nota's, evaluaties, verslagen, notulen, memo's en andere documenten over de reikwijdte en impact van de Patriot Act.
2. Advies-aanvragen en mededelingen van overheidsorganisaties, bedrijven en andere organisaties aan het ministerie van Binnenlandse Zaken over de reikwijdte en de impact de Patriot Act.
3. Het antwoord van het ministerie van Binnenlandse Zaken op onder de 2. genoemde documenten".

Bij brief van 11 september 2013 heb ik de ontvangst van uw verzoek aan u bevestigd.

Bij brief van 4 oktober 2013 is de termijn om op uw verzoek te beslissen met vier weken verlengd.

Op 31 oktober 2013 bent u uitgenodigd op mijn ministerie om met een aantal van mijn ambtenaren te spreken over uw verzoek. In dit gesprek heeft u uw verzoek toegelicht, dat u ook bij vijf andere ministeries heeft ingediend.

Van de kant van het ministerie is een toelichting gegeven op de summiere bij het Rijk beschikbare informatie over dit onderwerp en bent u gewezen op de beantwoording van vragen vanuit de Tweede Kamer. U heeft toegelicht dat uw verzoek geen betrekking heeft op de ambtelijke voorbereiding en totstandkoming van de beantwoording van de Kamervragen. U heeft aangegeven geïnteresseerd

te zijn in onderliggende documenten of rapporten in relatie tot casuïstiek. Van de vier onderwerpen die u in dit verband noemde heeft er slechts één betrekking op mijn ministerie. Aangezien u met betrekking tot dat onderwerp een afzonderlijk Wob-verzoek heeft ingediend, zal ik daarop bij afzonderlijk besluit een beslissing nemen.

Verder zijn onder meer afspraken gemaakt over de wijze en het moment van afdoening van uw verzoek.

**Datum**  
18 december 2013

**Kenmerk**  
2013-0000762191

In het kader van uw Wob-verzoek zijn de volgende documenten bij mijn ministerie aangetroffen.

Nr.	Omschrijving van het document	Openbaarmaking
1	Intern ambtelijk memo d.d. 26 juni 2013 aan minister voor WenR	nee
2	Verslag Kenniskring 15 maart 2013	ja
3	Ambtelijke e-mail d.d. 25 juni 2013 met verwijzing naar berichten in de pers (internet)	ja

Het interne ambtelijk memo verstrek ik u niet.

Dit document is opgesteld ten behoeve van intern beraad binnen mijn ministerie en bestaat uit persoonlijke beleidsopvattingen van de opsteller (ambtenaar), waarover op grond van artikel 11, eerste lid, van de Wob geen informatie wordt verstrekt. Voor zover in dit memo daarnaast feiten zijn opgenomen, zijn deze dermate nauw verweven met de persoonlijke beleidsopvattingen dat het niet mogelijk is deze van elkaar te scheiden, zodat ook hierover geen informatie wordt verstrekt.

Het verslag van de kenniskring, die eenmalig bijeen is geweest ter bespreking van het onderwerp Patriot Act, en de ambtelijke e-mail van 25 juni 2013 maak ik openbaar.

U zult zien dat enkele gegevens onleesbaar zijn gemaakt. Dit betreft in het verslag de (voor)namen van de aanwezigen en van de verslaglegger evenals zijn directe contactgegevens zoals e-mailadres en telefoonnummer, en in het e-mailbericht de (voor)namen van de opsteller en de geadresseerde van de e-mail (individuele ambtenaren) en hun directe contactgegevens zoals e-mailadressen. Deze gegevens maak ik niet openbaar in verband met de eerbiediging van de persoonlijke levenssfeer van betrokkenen, welk belang is opgenomen in artikel 10, tweede lid, aanhef en onder e, van de Wob. Dit belang afwegende tegen het belang van openbaarmaking van deze gegevens, acht ik het belang genoemd in artikel 10, tweede lid, aanhef en onder e, van de Wob zwaarwegender.

Tot slot deel ik u mee dat sprake is geweest van een door de Landsadvocaat uitgebracht advies. U heeft meegedeeld te accepteren dat dit advies niet wordt openbaar gemaakt. Zoals met u is afgesproken informeer ik u dat dit advies is gerelateerd aan de consolidatie van de datacenters van het Rijk (zie de Kamerstukken 31490, nrs. 119 en 117).

Dit Wob-besluit en de stukken die met dit besluit voor een ieder openbaar worden, zullen enkele werkdagen na toezending worden gepubliceerd op de website [www.rijksoverheid.nl](http://www.rijksoverheid.nl).

**Datum**  
18 december 2013

**Kenmerk**  
2013-0000762191

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,  
De minister van Binnenlandse Zaken en Koninkrijksrelaties,  
namens deze,

Richard van Zwol  
*Secretaris-generaal*

Bijlagen  
- verslag Kenniskring  
- e-mailbericht.

Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit daartegen per brief bezwaar maken bij de minister van Binnenlandse Zaken en Koninkrijksrelaties, Directoraat-generaal Organisatie en Bedrijfsvoering Rijk/Directie Informatiseringsbeleid Rijk, Postbus 20011, 2500 EA Den Haag. Het bezwaarschrift moet zijn ondertekend, voorzien zijn van een datum alsmede de naam en het adres van de indiener en dient vergezeld te gaan van de gronden waarop het bezwaar berust en, zo mogelijk, een afschrift van het besluit waartegen het bezwaar is gericht.



# verslag

## Kenniskring USA PATRIOT ACT

Programma CDC

Ministerie van Financiën  
Korte Voorhout 7  
2511 CW Den Haag

Vergaderdatum  
Deelnemers

15 maart 2013

[REDACTED] (RWS)  
[REDACTED] (PCDC)  
[REDACTED] (DJI)  
[REDACTED] (VenJ)  
[REDACTED] (DUO)  
[REDACTED] (EZ)  
[REDACTED] (Belastingdienst)  
[REDACTED] (EZ)  
[REDACTED] (SSC-ICT)  
[REDACTED] (VenJ)  
[REDACTED] (PCDC)  
[REDACTED] (PCDC)  
[REDACTED] (PCDC)

www.minfin.nl

Contactpersoon

Datum  
20 maart 2013

### Opening

[REDACTED] verwelkomt de aanwezigen bij deze Kenniskring-bijeenkomst in het teken van de USA PATRIOT ACT. Er bestaat behoefte aan verdieping op het onderwerp PATRIOT ACT ten behoeve van inzicht in risico's en mogelijkheden voor maatregelen. De Kenniskring PCDC heeft expert [REDACTED] gevraagd om haar ervaringen en kennis te delen. Ook andere geïnteresseerden buiten de Kenniskring zijn uitgenodigd. De doelstelling is om de aanwezigen verdiepende kennis en inzicht te laten verkrijgen over de PATRIOT ACT en aanverwante regelgeving. Tevens is de doelstelling de aanwezigen zoveel mogelijk in staat stellen deze kennis te gebruiken in relatie tot hun eigen casus. Naar aanleiding van deze bijeenkomst kunnen waar mogelijk en nuttig maatregelen worden getroffen in contracten met leveranciers. Deze bijeenkomst en de daarvoor rondgestuurde situatieschets over de PATRIOT ACT in relatie tot de Datacentervoorziening Rijk zullen dienen als basis voor een notitie aan de stuurgroep PCDC over dit onderwerp. Parallel aan deze bijeenkomst is de Landsadvocaat gevraagd een advies te geven over genoemde situatieschets.

### Presentatie [REDACTED]

[REDACTED] is partner bij De Brauw advocatenkantoor en expert op het gebied van grensoverschrijdende outsourcing van ICT en de daarbij behorende wet- en regelgeving zoals PATRIOT ACT en export controls. De (Rijks)overheid behoort niet tot haar klantenkring.

Als eerste wordt kort stilgestaan bij de vraag of er wetgeving bestaat om digitale rijksdata in eigen land op te slaan. Het antwoord daarop is "nee" en dat is volgens [REDACTED] opmerkelijk. Haar ervaring is dat landen veelal hun data op hun eigen grond willen opslaan en dit ook wettelijk verankeren.

Ze deelt ons in haar verbazing over het grote verschil in de wijze waarop de (Nederlandse) overheid en de multinationals in haar klantenbestand omgaan met risico's die verband houden met internationale wetten zoals de PATRIOT ACT en export controls. Bedrijven als Philips zijn bereid flink wat kosten te maken om met inzet van juristen hun bedrijfsgeheime en commercieel gevoelige data contractueel te beschermen. Hiertoe voeren zij harde onderhandelingen met hun ICT-dienstverleners. Voor zover [REDACTED] daarzicht op heeft, lijkt de overheid echter pas

na gunning op dit onderwerp contractueel maatregelen te treffen. Dat is praktisch onmogelijk gezien de slechte onderhandelingspositie die je dan hebt. Al in de aanloop naar en bij de publicatie van de aanbesteding zouden volgens haar strenge eisen gesteld moeten worden op het punt van databeveiliging.

**Datum**  
16 februari 2012

Volgens [REDACTED] is de ontwikkeling van cloud-diensten een katalysator geweest voor het professioneel denken over en verweren tegen informatiebeveiligings-risico's van internationale wetgeving. Dat blijkt onder meer uit bijvoorbeeld het feit dat het NCSC (Nationaal Cyber Security Centre) een bruikbaar rapport heeft opgesteld over dit onderwerp. Daarnaast heeft De Brauw samen met UWV gewerkt aan maatregelen die mogelijk herbruikbaar zijn binnen het Rijk. Een belangrijke doorbraak is de onderzoeksclausule (right to examine) die De Nederlandse Bank met Microsoft heeft afgesproken in verband met het gebruik van haar product Office 365. Overigens wordt rondom cloud-diensten en informatiebeveiliging op Europees niveau ook het een en ander ondernomen, maar dat is vooral gericht op de consumentenmarkt. Gericht op (Rijks)overheden sluit de ontwikkeling hieromtrent volgens [REDACTED] niet goed aan op de urgentie.

#### **USA PATRIOT ACT**

Belangrijke aspecten aan de PATRIOT ACT:

- De in 1978 vastgestelde Foreign Intelligence Surveillance Act (FISA) vormt in Amerika een wettelijke basis voor deze intelligence-activiteiten. Deze wet is in 2001 geamendeerd door de USA PATRIOT act waardoor er ook terroristische groeperingen onder vallen. Bovendien is in 2008 een amendement geweest onder meer gericht op cloud-serviceproviders.
- PATRIOT ACT is niet één wet, maar een verzameling van wetten.
- De PATRIOT ACT kan zelfs gelden voor Nederlandse bedrijven als deze een "nexus" (verbinding) hebben met een Amerikaans bedrijf. Van een dergelijke verbinding is sprake als een Amerikaans bedrijf rechtstreeks toegang heeft tot de data van het niet-Amerikaanse bedrijf of als het niet-Amerikaanse bedrijf een Amerikaans moederbedrijf heeft of als een Amerikaanse medewerker toegang heeft tot de data. In de praktijk zal in Amerika altijd geoordeeld worden dat er voldoende nexus is omdat geen Amerikaanse rechter dit zal bestrijden.
- Valt KPN (en dus het Overheidsdatacenter in Groningen) door de deelname van América Móvil nu onder de USA PATRIOT act? Nee, América Móvil is een Mexicaans bedrijf en valt dus niet onder de PATRIOT act. Bovendien – al zou het een Amerikaans bedrijf zijn – het aandeel van América Móvil in KPN is minder dan 30% waardoor de zeggenschap te klein is. De Nederlandse eigenaars van KPN zullen niet geneigd zijn in het kader van de PATRIOT act hun medewerkers informatie van de Nederlandse Overheid te laten doorgeven naar Amerika.
- De ontvanger van een NSL mag uitsluitend informatie verzamelen waar hij op basis van eigendom (*possession*), houderschap (*custody*) of beheer (*control*) rechtmatig beschikking over heeft. Met andere woorden: de betreffende persoon mag zich in principe niet via bijvoorbeeld inbraak toegang tot de informatie verschaffen. De Amerikaanse Overheid mag een individu of bedrijf dus niet aanzetten tot strafrechtelijke overtredingen. Het begrip control kan echter zeer breed worden uitgelegd: het feit dat iemand contractueel geen geautoriseerde toegang tot data op een server heeft, wil nog niet zeggen dat hij er geen control over kan hebben. Veel belangrijker hierbij is de vraag of deze persoon zich bij de uitvoering van de dienstverlening – gedwongen door Amerikaanse Overheid en in het verlengde daarvan zijn werkgever

(bijvoorbeeld op straffe van ontslag) – ongeautoriseerd toegang tot de data kan verschaffen. Als bijvoorbeeld een Amerikaans bedrijf in het kader van haar dienstverlening aan de Nederlandse overheid in de datacenterruimte moet komen en dus in de buurt kan komen van de dataservers, bestaat het risico dat

Datum  
16 februari 2012

hierbij – ondanks dat het volgens de contractafspraken niet mag – data wordt gekopieerd en meegenomen. Dit geldt ook bijvoorbeeld bij monitoring van netwerkverkeer waarbij een leverancier tegen contractafspraken in toch de inhoud van de data verzamelt in plaats van alleen de procesinformatie.

- Niet alleen Amerika heeft wetgeving die gericht is op het vergaren van intelligence-informatie. Er zijn ook Europese landen met vergelijkbare wetgeving. Belangrijk daarbij is dat Amerika fundamenteel andere opvattingen heeft over de rechten van burgers dan Europese landen.
- Van “control” is geen sprake als je bijvoorbeeld hardware koopt en die in eigen beheer neemt. Als je echter hardware koopt inclusief een onderhoudscontract daarop, kan de onderhoudsleverancier (vaak van afstand) bij de hardware en is dan wellicht in staat om (desnoods ongeautoriseerd) toegang te verschaffen tot de data.

### **Export controls**

Er is juridisch sprake van de export van data als deze de landsgrens overschrijden, bijvoorbeeld wanneer data opgeslagen in Amerika gestationeerde cloud-servers worden getransporteerd over de grenzen. In veel landen zijn er regels over de export van data. Op basis daarvan wordt gereguleerd dat andere landen niet ongewenst in het bezit kunnen komen van vertrouwelijke informatie. Deze regelgeving verschilt per land. Zo is het in Amerika bijvoorbeeld niet toegestaan om data te exporteren naar landen als Iran om te voorkomen dat bijvoorbeeld Amerikaanse kennis over de bouw van nucleaire wapens wordt gebruikt door Iran. Het kan zijn dat de Nederlandse overheid data bij bijvoorbeeld een cloudserviceprovider heeft ondergebracht die deze data in servers opslaat die op Amerikaans grondgebied staan. Als deze data vervolgens worden getransporteerd naar en gebruikt in een ander land, is er sprake van export van deze data. Het kan zijn dat dit tussen Amerika en dit andere land een exportverbod bestaat. In dat geval overschrijdt Nederland de Amerikaanse wet en riskeert dan forse boetes.

### **Afronding**

Op basis van de presentatie en discussie komen de aanwezigen tot de volgende constatering.

- Maatregelen die nu in Europees verband getroffen worden, zijn vooral gericht op consumentenmarkt. De Rijksoverheid zal zelf wat moeten regelen als ze zich wil beschermen in het kader van internationale informatiebeveiliging. Vertrouwen op privacywetgeving is onvoldoende;
- Het is een politiek risico als deze beveiliging onvoldoende wordt opgepakt vanwege onder meer de maatschappelijke onrust over dit onderwerp;
- Het is onder meer vanwege de kostenafweging van belang om te onderkennen dat er – ook in het kader van internationale informatiebeveiliging – verschillende soorten data zijn die om verschillende niveaus van beveiliging vragen. Maximale beveiliging voor alle data is praktisch onhaalbaar;
- Een vervolgbijeenkomst met UWV om te leren van hun ervaringen is zinvol;
- Ook in andere onderwerpen dan datacenters speelt de PATRIOT ACT, bijvoorbeeld bij (onderhouds)contracten op connectiviteit en hardware.
- Het onderwerp PATRIOT ACT raakt meerdere disciplines: ICT, inkoop, juridisch, informatiebeveiliging.

Afgesproken is dat het programma de vervolgssessie met UWV organiseert. Verder zal de stuurgroepnotitie over de PATRIOT ACT worden uitgewerkt. [redacted] zal binnen [redacted] aandacht vragen voor het feit dat dit onderwerp interdisciplinair en interdepartementaal gecoördineerd moet worden. Oproep aan de aanwezigen is tot slot om ter voorbereiding op het algemeen overleg met de Tweede Kamer vragen te bedenken die zouden kunnen worden gesteld over dit onderwerp en die van mogelijke antwoorden te voorzien.

Datum  
16 februari 2012

[REDACTED]

---

**Van:** [REDACTED]  
**Verzonden:** dinsdag 25 juni 2013 23:09  
**Aan:** [REDACTED]  
**CC:** [REDACTED]  
**Onderwerp:** equinix berichten

Ter info en voorbereiding AO.

<http://www.bnr.nl/nieuws/tech/243810-1306/overheid-huurt-cloud-in-amsterdam>

<http://www.apparata.nl/nieuws/overheid-huurt-amerikaans-datacentrum-niet-zo-slim-bezig-1885>

Gr [REDACTED]