

7 Bijlagen

Nummer	Naam	Pagina
1	Artikel website Trouw	34
2	Memo onderzoeksoopdracht	42
3	Instellingsbeschikking Commissie van Onderzoek	45
4	NLA Wob-verzoek Nieuwsuur / Trouw	48
5	Instructie Wob	58
6	Handleiding rubricering	70
7	VIRBI2013	79
8	Uitspraak RvS 201708297/1/A3 ECLI:NL:RVS:2019:100	94
9	E-mail informatie staatsgeheim in relatie tot de Wob	105
10	E-mail bijeenkomst taakgroep verdeling Wob-verzoeken	109



Bijlage 1

Artikel website Trouw

THEMA'S

HOME

RELIGIE EN FILOSOFIE

GROEN

DEMOCRATIE

SAMENLEVING

CULTUUR

OPINIE

SERVICE

KLANTENSERVICE

TROUW EXCLUSIEF

WEBWINKEL

DIGITALE KRANT

NIEUWSBRIEF

PUZZELS

ABONNEER JE NU

Staatsgeheimen over Nederlandse steun aan Syrische rebellen zijn per ongeluk onthuld

DEMOCRATIE

Ghassan Dahhan en Milena Holdert – 23:57, 21 november 2018



▲ Fragment uit een video van Jabhat al-Shamiya © x

Trouw en 'Nieuwsuur' onderzochten de afgelopen twee weken alle van de in totaal 1866 pagina's aan wob-documenten minutieus, en troffen daar opmerkelijke feiten aan. Hoewel de meeste documenten over het steunprogramma in Syrië zijn geweigerd, en het vrijgegeven deel ook nog eens veel zwartgelakte passages bevat, bleken de stukken per ongeluk staatsgeheime informatie te bevatten.

U krijgt 5 artikelen van Trouw cadeau. Dit is nummer 2 .

Onbeperkt onze artikelen lezen? Digitaal Basis € 2.50 per week.

De door Nederland gesteunde strijdgroepen en de twee uitvoerders – de bedrijven die de hulpgoederen namens Nederland aan de Syrische rebellen leverden – komen voor in de stukken, terwijl deze, bij navraag bij het ministerie van buitenlandse zaken, tot in ieder geval

gisteravond staatsgeheim waren. Ook informatie waaruit de namen van de groepen en bedrijven kon worden herleid, vielen onder deze categorie.

De Syrische strijdgroep Levant Front (Jabhat al-Shamiya) wordt meerdere keren genoemd in leveringsovereenkomsten (een keer in november 2017 en een keer in februari 2018). In een document komt zelfs een tevredenheidsonderzoek voor. Daaruit blijkt dat ‘100 procent’ van de strijders zeer tevreden is met de kwaliteit van het Nederlandse voedsel.

Trouw en Nieuwsuur onthulden al eerder, op basis van gesprekken met Syrische commandanten, dat deze strijdgroep Nederlandse steun ontving, maar Blok wilde dit ontkennen noch bevestigen. Het Nederlandse Openbaar Ministerie vervolgt op dit moment een Nederlandse man voor terrorisme omdat hij zich enkele jaren geleden zou hebben aangesloten bij Jabhat al-Shamiya. Volgens mensenrechtenorganisaties zoals Amnesty International heeft de groepering zich schuldig gemaakt aan mensenrechtenschendingen, waaronder het uitvoeren van standrechtelijke executies en het runnen van shariarechtbanken. Ook speelde de strijdgroep een rol bij de Turkse invasie in Afrin.

Zwartgelakt

Daarnaast komen nog twee andere groeperingen voor in de documenten, die nog niet eerder door Trouw en Nieuwsuur genoemd waren: de ‘Tweede Centrale Divisie’ en de ‘Hama Rebellen Gathering’. De laatste is onderdeel van het al vaker genoemde Jaish al-Nasr.

In de documenten komen ook de tot nu toe geheim gehouden namen van de ‘uitvoerders’ van het steunprogramma voor. Het gaat om het – al eens door Trouw en Nieuwsuur genoemde – Turkse bedrijf Candor International en het Amerikaanse Creative Associates, die namens Nederland goederen aan de rebellen leverden. Meestal zijn de bedrijfsnamen zwartgelakt, maar toch komen ze voor in de stukken,

CANDOR

INTERNATIONAL

102 g

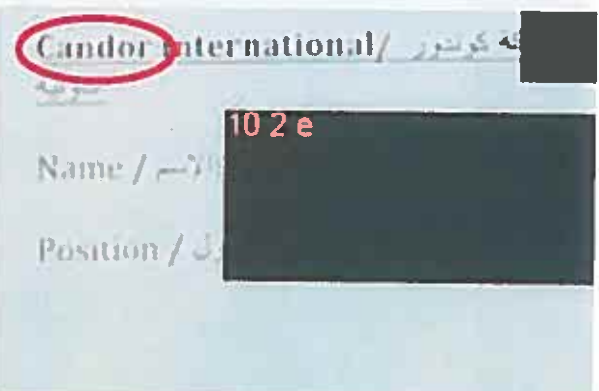
The vehicles will be based out of the head offices of 102 g and if it is moved to other provinces or countries, notice must be provided to Candor International

- In the event theft, confiscation and/or damage occurs to the vehicles, 102 g must immediately inform Candor International with an incident report.

soms met hun logo erbij.

Dat de informatie afkomstig is van het ministerie van buitenlandse zaken zelf brengt Blok in een lastige positie. De minister wilde de berichtgeving van Trouw en Nieuwsuur tot nog toe niet in het openbaar bevestigen omdat het bekendmaken van de namen van de door Nederland gesteunde Syrische strijdgroepen ‘mensenlevens op het spel’ zou zetten. En ondanks dat de commandanten zelf dit gevaar niet zagen en openlijk spraken over de Nederlandse hulp, zei Blok dat hij alsnog niets mocht zeggen vanwege ‘bondgenootschappelijke verplichtingen’ en de betrokkenheid van Nederlandse veiligheidsdiensten (AIVD en de MIVD) bij het steunprogramma.

Blok kon tot nu toe lastige vragen over het zogeheten NLA-programma ontwijken. Dat bleek ook deze week toen de minister vragen van CDA-Kamerlid Omtzigt over het Nederlandse steunprogramma moest beantwoorden. “Het kabinet doet geen uitspraken over namen en



De naam van het Turkse bedrijf Candor International (het bedrijf dat namens Nederland de goederen stuurde) is openbaar gemaakt.

locaties van gematigde gewapende groepen die het al-dan-niet heeft gesteund”, aldus Blok.

Nu zwart op wit staat dat Nederland ook daadwerkelijk een aantal groeperingen heeft gesteund, zal Blok moeten uitleggen waarom zijn ambtenaren de namen van gesteunde groeperingen geopenbaard hebben.

Dilemma

Als Blok vasthoudt aan het stempel staatsgeheim dan erkent hij dat hier fouten zijn gemaakt. Laat hij het stempel los, dan zal de Kamer hem vragen ook de andere namen van gesteunde groepen publiek te maken.

Op het onthullen van informatie die ‘staatsgeheim’ is verklaard, staat een flinke straf. Kamerleden van de commissie Buitenlandse Zaken, die in september de kans kregen om overheidsdocumenten vertrouwelijk in te zien over het Syrië-programma, moesten een geheimhoudingsverklaring tekenen. Daarin stond dat hun een gevangenisstraf van zes jaar boven het hoofd hing als zij informatie naar buiten zouden brengen.

Uit de opgevraagde stukken wordt duidelijk dat de veiligheidsdiensten nauw betrokken waren bij het steunprogramma. In de inventarislijst van het Wob-verzoek om alle documenten waarin het Nederlandse steunprogramma voorkwam, staan 27 geweigerde stukken met als beschrijving ‘veiligheidsdiensten/gespreksverslag’. Ook staat in een memo beschreven dat het NLA-programma van ‘onschatbare waarde’ is voor de ‘Nederlandse inlichtingenpositie’.

Al eerder bleek dat binnen het Nederlandse Syrieteam, dat het steunprogramma vanuit Turkije en Jordanie aanstuurde, ook een medewerker van de MIVD actief was. Hij bleek een van de belangrijkste contactpersonen van de Syrische rebellen, die hem allemaal kenden bij zijn voornaam.

Wat is er nou gebeurt met de voedselpakketten?

Minister Blok meldde vorige maand dat gedurende het gehele NLA-programma in totaal twee incidenten hadden plaatsgevonden, waarin Nederlandse goederen in handen waren gevallen van extremisten. Het eerste incident vond plaats in november 2015, toen Al-Qaida in totaal 1800 Nederlandse voedselpakketten in beslag nam die bedoeld waren voor ‘gematigde

strijders'. Het tweede incident vond plaats in maart 2017, toen de terreurbeweging een Nederlandse mobiele oven in handen kreeg.

Bij de overval in 2015 door Al-Qaida zijn nog veel vragen onopgehelderd. De toenmalige minister van buitenlandse zaken Bert Koenders zei dat de voedselpakketten na bemiddeling zouden zijn teruggegeven. Maar uit de wob-documenten blijkt dat nooit te zijn vastgesteld. Er waren twijfels over het verhaal van de door Nederland gesteunde commandant. Hij stuurde beelden op van de 'teruggegeven' voedselpakketten maar deze waren niet voorzien van 'tijdsaanduiding, locatie en de flyer'.

De Nederlandse regering maakte indertijd zich grote zorgen over de ophef die het incident zou kunnen teweegbrengen als het naar buiten kwam, vanwege de flyer op de voedselpakketten. Daarop stond 'Donatie van Nederland' met de Nederlandse vlag. De regering wilde geen ruchtbaarheid aan de zaak geven en koos voor een 'passieve woordvoering'.

Er blijkt echter nog een derde incident te hebben plaatsgevonden dat nog niet eerder was gemeld door de regering, ook niet na Kamervragen. In mei 2016 raakten door Nederland gesteunde groeperingen een vijftigtal dekens en nog een aantal matten kwijt in de strijd tegen terreurbeweging Islamitische Staat (IS). Volgens het verslag zijn de goederen waarschijnlijk in handen gekomen van de groepering.

Lees ook:

Tweede Kamer wil minister Blok opnieuw spreken over militaire steun aan Syrische rebellen

De Tweede Kamer gaat binnenkort in debat over de voor de strijd bedoelde goederen die Nederland aan Syrische rebellen heeft geleverd. Het verzoek om een debat van SP-Kamerlid Sadet Karabulut kreeg donderdagmiddag steun van de gehele Tweede Kamer.

Waarom wij staatsgeheimen publiceren

Trouw en Nieuwsuur publiceerden uit documenten die door het ministerie van buitenlandse zaken zijn vrijgegeven na een wob-verzoek. Een deel van de informatie daarvan is staatsgeheim, maar per abuis niet onleesbaar gemaakt. Volgens de minister was het noodzakelijk gegevens over het Nederlandse hulpprogramma aan Syrische rebellengroepen

tot staatsgeheim te verklaren omdat er bij publiciteit daarover levens in gevaar kunnen komen. Toch publiceerden we. De hoofdredactie van Trouw legt uit waarom.

De Nederlandse hulp aan Syrië was wel militair van aard

Nederlandse hulpgoederen aan Syrische rebellen zijn wel degelijk militair ingezet. Minister Blok weersprak dit eerder.

Hoe Al-Qaida aan een mobiele bakkerij uit Nederland kwam

Hoe kwam de omstreden hulp aan Syrische strijdgroepen daar eigenlijk terecht, en wat gebeurde ermee? Trouw en Nieuwsuur brachten het logistieke proces in kaart, voorafgaand aan het Kamerdebat vandaag. Er ging veel mis.

UITGELICHT | NET BINNEN



Ook met de belofte af te treden krijgt premier May het Lagerhuis niet achter zich

DEMOCRATIE

De Britse premier belooft te vertrekken als het Lagerhuis instemt met haar plan. Voor de alternatieven blijkt niet genoeg steun.



Bijlage 2

Memo onderzoeksopdracht



Aan SG
Van BVA
Via
Kopie aan DJZ, DGPZ
Afgestemd met DJZ

TER BESLISSING

Datum
27-11-2018

Onze Referentie
ENV-2018 6183

Opgesteld door
[...]

T [...]

memo

Verzoek instellen Commissie van onderzoek inzake WOB
verzoek NLA

Aanleiding

Op 26 november 2018 deed de plv. directeur Directie Midden-Oosten en Noord-Afrika melding bij mij als Beveiligingsambtenaar dat er Stg gerubriceerde informatie via een WOB-procedure over *non-lethal assistance* (NLA) openbaar is gemaakt.

Gevraagd besluit

Instelling van Commissie van onderzoek middels tekenen van bijgevoegde instellingsbeschikking.

) d.w. 27/11

Kern/samenvatting

In de, middels een WOB-verzoek verkregen, gepubliceerde informatie blijkt gerubriceerde informatie vermeld te staan. Hierdoor is er sprake van compromittatie van gerubriceerde informatie zoals beschreven in Rijksbreed Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013).

Ik zie op dit moment, geen aanleiding tot een redelijk vermoeden dat strafbare feiten zijn gepleegd. Indien tijdens het onderzoek dit beeld verandert, zal het onderzoek worden stopgezet en zal er, in nauwe samenspraak met u, vervolgstappen worden bepaald.

Dit onderzoek is geen persoonsgericht onderzoek.

DGPZ is reeds geïnformeerd over dit advies.

Toelichting

Bij de publicatie van het WOB-verzoek over NLA zijn bijna 2000 pagina's vrijgegeven waarin gevoelige informatie is weggelakt, echter op een aantal plekken bleken de namen van NLA-ontvangende groepen ten onrechte niet te zijn weggelakt. Elementen van het NLA-programma zijn sinds de start van het programma STG-confidentieel gerubriceerd ter beveiliging van de groepen, betrokkenheid van bondgenoten en betrokkenheid van inlichtingendiensten. Inmiddels heeft de Directie Midden-Oosten en Noord-Afrika onmiddellijke noodmaatregelen getroffen door de WOB-bijlagen offline te halen.

Er was tevens sprake van een datalek. Dit betrof de naam van een medewerker van de MIVD. Dit datalek is op 22 november gemeld bij de Autoriteit Persoonsgegevens (AP). De betrokken persoon is, conform de AVG, geïnformeerd.

Basis voor het onderzoek vormen de artikelen 8 en 9 van het Voorschrift Informatiebeveiliging Rijksdienst (VIRBI) 2013:

Artikel 8 Compromittering van bijzondere informatie

1. Elke ambtenaar is verplicht de Beveiligingsambtenaar (BVA) onmiddellijk mededeling te doen van een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van bijzondere informatie.
2. De BVA laat, nadat hij op de hoogte is gebracht van een inbreuk op de beveiliging, onmiddellijk (nood)maatregelen treffen om verdere inbreuk te voorkomen.
3. De BVA onderzoekt of compromittering van bijzondere informatie heeft plaatsgevonden; indien dit het geval is doet hij hiervan mededeling aan de secretaris-generaal en adviseert over de noodzaak tot het instellen van een commissie van onderzoek.
4. Indien de compromittering betrekking heeft op bijzondere informatie die is verkregen van een ander ministerie of krachtens Internationaal verdrag of overeenkomst, doet de BVA bovendien mededeling aan dat betreffende ministerie of de krachtens het verdrag of de overeenkomst voor de beveiliging van die bijzondere informatie verantwoordelijke instantie.

Artikel 9 Commissie van onderzoek

1. Een commissie van onderzoek wordt ingesteld door de secretaris-generaal.
2. De commissie stelt een onderzoek in naar:
 - a. de wijze waarop de compromittering heeft plaatsgevonden;
 - b. de aard en de omvang van de schade aan de belangen van de Staat of zijn bondgenoten;
 - c. de te nemen maatregelen om de schade te beperken en herhaling te voorkomen.
3. De commissie voert, indien de gecompromitteerde bijzondere informatie (mede) afkomstig is van een ander ministerie, haar onderzoek uit in overleg met de BVA van dat ministerie. In het geval dat de gecompromitteerde bijzondere informatie krachtens een internationaal verdrag of overeenkomst is verkregen voert de commissie haar onderzoek uit in samenwerking met de instantie die krachtens het verdrag of de overeenkomst verantwoordelijk is voor de beveiliging ervan.
4. De secretaris-generaal of een door hem aangewezen ambtenaar treft, op basis van de bevindingen van de commissie van onderzoek, maatregelen om de schade die de compromittering heeft toegebracht aan de veiligheid of andere gewichtige belangen van de Staat of zijn bondgenoten te beperken en herhaling van de compromittering te voorkomen.
5. Indien het de compromittering van een staatsgeheim betreft stelt de secretaris-generaal het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst in kennis van de uitkomsten van het onderzoek. Bij het ministerie van Defensie wordt de Militaire Inlichtingen- en Veiligheidsdienst op de hoogte gesteld van de uitkomsten van het onderzoek.

Bijlage:

- instellingsbeschikking Commissie van onderzoek



Bijlage 3

Instellingsbeschikking Commissie van Onderzoek

Instellingsbeschikking Commissie van Onderzoek

Datum
27-11-2018
Onze Referentie

De Secretaris-Generaal van het Ministerie van Buitenlandse Zaken,

overwegende dat:

- bij de publicatie van het WOB-verzoek over NLA bijna 2000 pagina's zijn vrijgegeven waarbij ongeveer 25.000 tot 30.000 lakhandelingen zijn gepleegd;
- op een aantal plekken de namen van NLA-ontvangende groepen en de ingeschakelde uitvoerders niet ~~te~~ zijn weggelakt;
- elementen van het NLA-programma sinds de start van het programma STG-confidentieel zijn verklaard vanwege veiligheid van de groepen, betrokkenheid van bondgenoten en betrokkenheid van inlichtingendiensten.

besluit tot:

- instelling van een Commissie van onderzoek conform gestelde in artikel 9 Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzonder Informatie (VIRBI 2013)

De commissie van onderzoek bestaat uit de volgende VCI medewerkers:

- voorzitter: Arjen Mostert (VCI-onderzoeker)
- [...] (coördinator Veiligheidscluster)
- [...] (medewerker Veiligheidscluster)
- [...] (Integriteitscoördinator)
- [...] (VCI-onderzoeker)
- [...] (medewerker Integriteitscluster)
- [...] (medewerker fysieke – en informatiebeveiliging)

De commissie kan in wisselende samenstelling onderzoekshandelingen uitvoeren. Onderzoekshandelingen worden altijd uitgevoerd door ten minste twee onderzoekers samen.

De commissie stelt een onderzoek in naar:

- a. de wijze waarop de compromittering heeft plaatsgevonden;
- b. de aard en de omvang van de schade aan de belangen van de Staat of zijn bondgenoten;
- c. de te nemen maatregelen om de schade te beperken en herhaling te voorkomen.
- De commissie zal tevens aandacht besteden aan de context waarbinnen dit heeft kunnen plaatsvinden.

De commissie is bevoegd om:

- Onderzoekshandelingen te verrichten die noodzakelijk zijn, zoals het interviewen van medewerkers en evt. derden, onderzoek naar ter beschikking gestelde (e-mail)correspondentie en documenten en het raadplegen van dossiers.
- Indien het noodzakelijk is om ook onderzoek aan apparatuur die ter beschikking is gesteld (bijv. gebruik van internet, pc, mailverkeer) uit te voeren zal separaat toestemming aan mij worden verzocht.

Datum
27-11-2018

Onze Referentie

Iedere ambtenaar van BZ is gehouden zijn of haar medewerking te verlenen aan het onderzoek.

De commissie streeft er naar haar onderzoek af te ronden voor 1 maart. De commissie zal mij tijdig, uiterlijk voor 22 februari, informeren indien deze deadline niet haalbaar blijkt.

Indien tijdens het onderzoek een redelijk vermoeden ontstaat van een strafbaar feit, staakt de commissie het onderzoek en word ik door de BVA geïnformeerd.

Den Haag, 27 november 2018

Ministerie van Buitenlandse Zaken,
De Secretaris-Generaal,

Joke Brandt



Bijlage 4

NLA Wob-verzoek Nieuwsuur / Trouw

Televisieprogramma *Nieuwsuuren* dagblad *Trouw*

NTR - redactie *Nieuwsuur*

t.a.v. naam

verwijderd

NOS-gebouw

Journaalplein 1

1217 ZK Hilversum

Ministerie van Buitenlandse Zaken

Rijnstraat 8

2515XP Den Haag

Amsterdam, 22juni2018

Betreft: Wob-verzoek non-lethal assistance (NLA)

Geachte heer/mevrouw,

Hierbij doen wij namens het programma *Nieuwsuur* en dagblad *Trouw* een verzoek om toezending van informatie met betrekking tot de Nederlandse steun aan gematigde gewapende oppositiegroepen in Syrie, oftewel het *non-lethal assistance*-programma (NLA). Daarbij verzoeken wij u in ieder geval afschriften van de volgende stukken toe te zenden:

- Een zo volledig en compleet mogelijk overzicht van alle goederen, gelden en/of diensten die Nederland (al dan niet via derden) in het kader van het NLA-programma tussen 1 januari 2011 en 22 juni 2018 naar Syrie heeft gestuurd, onderverdeeld in specifieke categorieën per geleverd goed en/of dienst (dus niet alleen algemene, overkoepelende termen zoals 'communicatiemiddelen', 'uniformen' of 'voertuigen' maar een zo specifiek mogelijke beschrijving van het type en soort product en/of dienst inclusief de bijbehorende productspecificaties zoals serienummers, jaartal van productie, uiterlijke kenmerken, enzovoorts), met daarbij per categorie het precieze aantal weergevend van geleverde zaken en/of goederen, een uitsplitsing van de financiële waarde en kosten, de betreffende

- producent en/of (toe)leverancier en/of uitvoerder van het product en/of dienst en de herkomst van het product en/of dienst
- Een zo volledig en compleet mogelijk overzicht van alle goederen, gelden en/of diensten die Nederland in het kader van het NLA-programma tussen 1 januari 2011 en 22 juni 2018 heeft overwogen om naar Syrië te sturen
 - Een zo volledig en compleet mogelijk overzicht van alle goederen, gelden en/of diensten die via (een) non-lethal assistance-programma('s) (van derden dan wel buitenlandse partners) tussen 1 januari 2011 en 22 juni 2018 naar Syrië zijn gestuurd waarbij Nederland op enigerlei wijze een (faciliterende dan wel doorvoerende dan wel uitvoerende) rol heeft gespeeld
 - Alle documenten (inclusief maar niet uitsluitend (concept)-verslagen, berichten, correspondentie, notulen, notities, rapporten, onderzoeken, evaluaties, analyses, aanbestedingen, projectbeschrijvingen, contracten, adviezen, resultaten en rapportages) over de periode tussen 1 januari 2011 en 22 juni 2018 die betrekking hebben op het NLA-programma
 - Alle documenten (inclusief maar niet uitsluitend (concept)-verslagen, berichten, correspondentie, notulen, notities, rapporten, onderzoeken, evaluaties, analyses, adviezen, resultaten en rapportages) over de periode tussen 1 januari 2011 en 22 juni 2018 die betrekking hebben op dan wel ten grondslag liggen aan de besluitvorming omtrent het NLA-programma dan wel op enigerlei wijze de basis vormen van de argumentatie en/of redenen waarom Nederland het besluit nam om (non-lethale) steun te gaan leveren aan groeperingen in Syrië
 - Alle documenten die een overzicht bevatten of gewag maken van de eerste specifieke datum waarop Nederland de beslissing nam niet-lethale steun aan oppositiegroepen in Syrië te leveren
 - Alle documenten die een overzicht bevatten of gewag maken van de eerste specifieke datum waarop Nederland de eerste (lading) niet-lethale steun (indirect dan wel direct) naar Syrische oppositiegroepen stuurde
 - Bijlage nummer 10 in het aanhangsel van de Handelingen nr. 953 gepubliceerd op 25 januari 2018

- Een overzicht van de door Nederland gemaakte kosten en uitgaven betrekking hebbend op het NLA-programma in de periode tussen 1 januari 2011 en 22 juni 2018
- Alle documenten die betrekking hebben op zowel het genoemde NLA-programma als op al dan niet verstrekte vergunningen in het kader van (nationale dan wel internationale) wetgeving omtrent wapenexport
- Alle documenten die betrekking hebben op (de) uitvoerende organisatie(s) die de NLA-steun aan gematigde gewapende groepen in Syrië heeft/hebben geleverd tussen 1 januari 2011 en 22 juni 2018. Hierbij citeren wij uit een Kamerbrief (Kamerstuk 27925 nr. 534) waarin het ministerie van Buitenlandse Zaken gewag maakt van een dergelijke organisatie: 'In totaal wordt voorzien in een steunpakket van 3 miljoen euro, gefinancierd uit het Stabiliteitsfonds, dat door een uitvoerende organisatie aan verschillende gematigde gewapende groepen geleverd kan worden in zowel Noord- als Zuid-Syrië.'
- Alle documenten die betrekking hebben op de *vetting-procedure* (inclusief maar niet uitsluitend de daarbij gehanteerde criteria) van partners (zoals Amerika) waar het ministerie van Buitenlandse Zaken in openbare Kamerstukken meermaals naar verwijst in het kader van de selectie van gewapende groepen in Syrië voor het NLA-programma. Wij noemen bijvoorbeeld Kamerstuk 27925 nr. 534 waarin de minister van Buitenlandse Zaken schrijft: 'Om te beginnen neemt het kabinet groepen in overweging die door partners - aan de hand van een zogenoemde *vetting-procedure* - als voldoende betrouwbaar zijn beoordeeld.'
- Alle documenten die betrekking hebben op de Nederlandse *vetting*- dan wel selectieprocedure (inclusief maar niet uitsluitend de daarbij gehanteerde criteria) waar het ministerie van Buitenlandse Zaken in openbare Kamerstukken meermaals naar verwijst in het kader van de selectie van gewapende groepen in Syrië binnen het NLA-programma. Wij citeren opnieuw Kamerstuk 27925 nr. 534: 'In aanvulling op deze voorselectie hanteert het kabinet een eigen *vetting-procedure*, die erin voorziet groepen te toetsen aan een aantal voor het kabinet doorslaggevende criteria.'

- Alle documenten over de periode tussen 1 januari 2011 en 22 juni 2018 die betrekking hebben op zowel het Stabiliteitsfonds als op het NLA-programma
- Alle documenten die betrekking hebben op de wijze waarop Nederland de goederen, diensten en/of financiële transacties in het kader van het genoemde NLA-programma volgt en/of monitort. Hierbij verwijzen wij naar een uitspraak van de minister van Buitenlandse Zaken in een verslag van een Algemeen Overleg, vastgesteld op 2 maart 2015 (Kamerstuk 27925 nr. 531): 'We maken het geld uiteraard niet alleen over, maar kijken ook wat ermee gebeurt.'
- Alle documenten die betrekking hebben op de monitoring (inclusief maar niet uitsluitend de daarvoor verantwoordelijke uitvoerende organisatie(s)) van het NLA-programma. Hierbij verwijzen wij naar een citaat van de minister van Buitenlandse Zaken (Kamerstuk 27925 nr. 534): 'Aan het leveren van steun zijn tevens andere risico's verbonden, die van belang zijn voor de afweging van het kabinet. Het risico op fraude wordt geadresseerd door professionele *monitoring* en door het gebruik van overdrachtsbewijzen van goederen. Daarbij kan door toenemende instabiliteit in de toekomst sprake zijn van verminderde uitvoerbaarheid in de grensregio's. En niet in de laatste plaats lopen de medewerkers van de uitvoerende organisatie - in het bijzonder degenen die naar Syrie reizen - persoonlijke risico's bij het leveren van steun aan gewapende groepen. Dit risico wordt gemitigeerd door te werken met een ervaren organisatie die, op basis van eerdere werkzaamheden bij andere donoren, een goede reputatie heeft. De uitvoerende organisatie werkt vanuit Turkije en Jordanië. De betreffende autoriteiten zijn inmiddels ingelicht.' Wij verzoeken tevens om de overdrachtsbewijzen al dan niet met geanonimiseerde namen van medewerkers
- Alle documenten over de periode tussen 1 januari 2011 en 22 juni 2018 die betrekking hebben op dan wel voortvloeien uit het driemaandelijks weegmoment waarbij de positie en effectiviteit van de door Nederland gesteunde oppositiegroepen in Syrie wordt gewogen. Wij verwijzen hiervoor naar een Kamerbrief van 11 september 2017 (Kamerstuk 27925 nr. 612), waarin de

minister van Buitenlandse Zaken schrijft: 'Elke drie maanden is een weegmoment waarbij de positie en effectiviteit van groepen en de algehele situatie in Syrie warden beoordeeld, om te bepalen of voortzetting van het programma nog effectief en wenselijk is gezien de context.' Ook verwijzen wij naar dit citaat uit de Kamerbrief van Buitenlandse Zaken van 17 mei 2018 (Kamerstuk 32623, nr. 218): 'Het steunprogramma aan de Syrische gewapende oppositie wordt doorlopend gemonitord en elke drie maanden, voorafgaand aan een nieuwe financiële bijdrage, geevalueerd.'

- De externe evaluatie van het NLA-programma en alle documenten die daarop betrekking hebben, inclusief conceptversies van de evaluatie. De minister verwijst naar deze evaluatie in een Verslag van een Schriftelijk Overleg, vastgesteld op 30 mei 2018 (Kamerstuk 32623 nr. 219): 'Het steunprogramma aan de Syrische gewapende oppositie wordt doorlopend gemonitord door Nederland en door de uitvoerders van de programma's. Ook heeft een externe evaluatie plaatsgevonden.'
 - Alle documenten met betrekking op civiele goederen dan wel civiele diensten die Nederland in de periode tussen 1 januari 2011 en 22 juni 2018 direct dan wel indirect aan groepen in Syrie heeft geleverd
 - Alle documenten met betrekking op dual use-goederen dan wel dual use-diensten die Nederland in de periode tussen 1 januari 2011 en 22 juni 2018 direct dan wel indirect aan groepen in Syrie heeft geleverd
 - Alle documenten met betrekking op militaire goederen dan wel militaire diensten die Nederland in de periode tussen 1 januari 2011 en 22 juni 2018 direct dan wel indirect aan groepen in Syrie heeft geleverd
 - Alle documenten met betrekking op wapens die in de periode tussen 1 januari 2011 en 22 juni 2018 zijn geëxporteerd met eindbestemming Syrie waarbij Nederland op de een of andere manier een rol heeft gespeeld, indirect dan wel direct, in faciliterende, producerende, leverende, controlerende of andere
- Zin

_ Alle documenten tussen 1 januari 2011 en 22 juni 2018 die betrekking hebben op de verzorging van het transport door Nederland van wapens die door Oost-Europese landen en Duitsland beschikbaar worden/werden gesteld aan/naar (individuen, groeperingen, overheden, bedrijven en/of organisaties in) Syrië, Jordanië, Turkije en/of Irak (Kamerbrief DVB/CV-169/2014)

_ En alle overige stukken die betrekking hebben op deze aangelegenheid.

Dit verzoek doen wij op basis van de Wet openbaarheid van bestuur (Wob). Daaruit vloeit voort dat u binnen 4 weken een besluit moet nemen op dit verzoek.

Gegeven de overzichtelijkheid van dit verzoek en het journalistieke belang verzoeken wij u zo spoedig mogelijk, doch uiterlijk binnen 28 dagen na dagtekening van dit verzoek te beslissen en geen gebruik te maken van de wettelijke verdagingsmogelijkheid.

Indien de verzochte informatie niet op schrift is vastgelegd maar mondeling of anderszins is gedocumenteerd verzoeken wij u deze informatie te verzamelen en op schrift te stellen teneinde ons haar schriftelijk te doen toekomen.

In het geval dat (delen van) de door ons verzochte informatie bij andere ministeries dan wel bestuursorganen dan wel overheidsorganisaties (inclusief maar niet uitsluitend ambassades en het Nederlandse Syrië-team) aanwezig is/zijn vragen wij u ons verzoek aan die betreffende organen door te geleiden. Indien deze documenten zich niet bij een bestuursorgaan bevinden dan verzoeken wij u om deze documenten op te vragen om daar vervolgens op te beslissen.

Macht u nog een nadere toelichting wensen op dit verzoek dan kunt u uiteraard contact met ons opnemen. Wij danken u bij voorbaat voor de aan dit verzoek te besteden aandacht.

In afwachting van uw antwoord, verblijven wij,

Hoogachtend namens *Nieuwsuuren Trouw*,

Naam verwijderd

Redacteur *Nieuwsuur*

tel.nr. verwijderd

naamverwijderd@nieuwsuur.nl

Naam verwijderd

Redacteur Trouw

tel.nr. verwijderd

naamverwijderd@trouw.nl

Ministerie van Buitenlandse Zaken

*Rijnstraat 8
2515 XP Den Haag*

ING KOMEN 27 JUNI 2018



NTR redactie Meursum
t.a.v. [...]

Journal plein 1

12 17 2k Hilversum

078 p1ee1aq llUlljUeJl IN
H
::1:1118 :JON:D:119NVV

INSON
-V-O



Bijlage 5
Instructie Wob

Behandeling Wob-verzoeken BZ

Inhoud

Procesbeschrijving behandeling Wob-verzoeken en verdeling verantwoordelijkheden	2
Behandelen van Wob-verzoeken.....	3
1. Inventarisatie documenten.....	3
2. Beoordeling documenten	3
3. Reactie aan Verzoeker: het Wob-besluit	3
4. Format inventarislijst documenten.....	3
Praktische tips.....	4
Uitzonderingsgronden –Artikelen 10 en 11 Wob	5
Toelichting uitzonderingsgronden.....	7
BZ-instructie digitaal lakken bij Wob-verzoeken	10

Procesbeschrijving behandeling Wob-verzoeken en verdeling verantwoordelijkheden

DJZ

- registreert Wob-verzoek in Sophia en Wob-plaza.
- Stuurt verzoek naar post/directie ter behandeling en stuurt cc aan betrokken SG/PSG/DG.
- Informeert in overleg met beleidsafdeling M/R gevoelige Wob-verzoeken d.m.v. bulletin.
- Stuurt verzoek vanuit media ter info aan COM.
- Adviseert de directie/post over afhandeling Wob-verzoek.

Directie/post

- Dossierhouder is verantwoordelijk voor afhandeling verzoek en wijst medewerker aan die coördineert en verantwoordelijk is voor:
- Verzamelen stukken en maken inventarislijst (zie format);
- Werkafspraken met betrokken directies, zo nodig in een startbijeenkomst;
- Beoordelen documenten aan criteria Wob;
- Scannen en lakken stukken.

Directie/post

- Stuurt verdaagbrief indien besluit nemen in 4 weken niet lukt (er kan eenmalig met 4 weken verdaagd worden).
- Vraagt, indien van toepassing, zienswijze aan derden.
- Stelt conceptbesluit op, met ondersteuning van DJZ.
- Legt gevoelige besluiten ter informatie of, ter instemming voor aan M of R.
- Ondertekent besluit namens M/R door tekeningsbevoegde.

Directie/post

- Zorgt voor verzending besluit aan verzoeker.
- Archiveert besluit met bijlagen.
- Archiveert stukken die niet openbaar zijn gemaakt.
- Leverit digitaal kopie verzonden besluit en openbaar gemaakte stukken aan bij DJZ ter plaatsing op rijksoverheid.nl.

Directie/post/DJZ/COM
BSG

- Voeren tussentijds overleg bij bijzonderheden zoals:
- opportuniteit gesprek met verzoeker;
- politiek/mediagevoelige besluiten ;
- verzoeken waarbij informatie bij meerdere directies/posten is belegd.
- Bij onduidelijkheid of frictie over verantwoordelijkheden wordt z.s.m. opgeschaald.
- Modelbrieven en meer informatie over de Wob staan op HBBZ.
- Bij interdepartementale Wob-verzoeken vindt interdepartementale afstemming plaats.
- Het behandelen van Wob verzoeken is maatwerk. Indien nodig wordt van bovenstaand schema afwegweten.

Behandelen van Wob-verzoeken

De Wet openbaarheid van bestuur (Wob) geeft aan iedereen het recht om overheidsdocumenten op te vragen. Het begrip overheidsdocumenten is breed en omvat ook digitale stukken, zoals e-mails. Het uitgangspunt is dat alle overheidsdocumenten openbaar zijn, tenzij er een uitzonderingsgrond van toepassing is. In reactie op een Wob-verzoek dient BZ een besluit te nemen. Aan de Wob zijn termijnen gebonden: er moet besloten worden binnen 4 weken. Dit kan eenmalig verlengd worden met nog eens 4 weken. De verantwoordelijkheid voor het afhandelen van Wob-verzoeken bij BZ is decentraal belegd: de directie of post die gaat over het dossier waarover het Wob-verzoek gaat, verzamelt dus ook de relevante stukken, beoordeelt deze en ondertekent het besluit namens M of R. DJZ ondersteunt dit proces juridisch.

1. Inventarisatie documenten

De documenten waar verzoeker om vraagt, worden geïnventariseerd en verzameld door de dossierhouder. Van deze documenten wordt een inventarislijst gemaakt conform onderstaand format. In dit overzicht wordt ook opgenomen of documenten geheel/gedeeltelijk of niet openbaar worden gemaakt.

2. Beoordeling documenten

Niet alle gevraagde documenten hoeven te worden gegeven. Er zijn uitzonderingen op de verplichting tot openbaarmaking (de uitzonderingsgronden staan in artikelen 10 en 11 van de Wob, zie de hoofdstukken 'Uitzonderingsgronden' en 'Toelichting uitzonderingsgronden').

3. Reactie aan Verzoeker: het Wob-besluit

Uiteindelijk moet er een brief uitgaan naar verzoeker, het Wob-besluit. Dit is het besluit of informatie wel of niet openbaar is, met daarbij een motivering (ondertekening namens M of R).

4. Format inventarislijst documenten

Nummer	Datum	Naam document	Beoordeling Wob (met artikelnummers)
1	12-09-2016	Memo aan M 'Stand van zaken'	Gedeeltelijk openbaar 10,2, a en 11 Wob
2	14-09-2016	Verslag gesprek SG	Niet openbaar, 11 Wob
3 etc.	15-09-2016	Mailwisseling	Openbaar

Dit is een format in een Word-tabel. Er kan vanzelfsprekend ook gewerkt worden met Excel, dit is met name handig als het gaat om veel documenten. Stel vanaf het begin (in overleg met andere medewerkers/departementen) een format op voor de bestandsnamen en de inventarissen. Dit bespaart veel tijd als er verschillende medewerkers documenten aanleveren. Als meerdere mensen documenten aanleveren kan het veel tijd besparen als alle documenten volgens hetzelfde format namen krijgen. Handig hierbij kan zijn de datum erin te zetten (2016-05-22 – Gespreksfiche M en dhr. X), op die manier zijn stukken makkelijk uit elkaar te houden en kunnen op die manier (in Excel) automatisch gesorteerd worden in een inventaris.

Praktische tips

Beoordeling documenten: Spreek af hoe de beoordeling van de documenten zal worden gedaan: hoeveel mensen moeten hiernaar gekeken hebben, en op welk niveau? Denk hierbij ook aan mogelijk andere directies of andere departementen. Houd hier rekening mee bij tijdsplanning.

Capaciteit: Het is niet altijd goed te voorspellen hoeveel tijd een Wob-verzoek zal vergen (onduidelijk hoeveel relevante documenten, etc.). Maak goede afspraken met je leidinggevende over de mogelijkheid voor extra ondersteuning, voor bijvoorbeeld het weglakken van passage/afdrukken/inscannen.

Niet uitstellen/onderschatten: Begin snel met de inventarisatie van mogelijk relevante documenten. Er kunnen altijd weer nieuwe typen documenten opduiken, het kan tijd kosten contact op te nemen met alle betrokken medewerkers. Trek als beleidsmedewerker op tijd aan de bel als een eerste inventarisatie oplevert dat het verzoek veel werk gaat kosten en er daarom extra handen nodig zijn.

Prioriteit stellen: Wob-verzoeken en verzoeken aan collega's om hiervoor stukken aan te leveren hebben de neiging onderaan to-do-lijstjes te blijven staan. Spreek anderen aan op hun verantwoordelijkheid en schroom niet je leidinggevende hiervoor in te schakelen als dat nodig is.

Neem tijd voor afstemming: er kan veel tijd gaan zitten in stukken die door andere directies/departementen moeten worden gezien, zeker andere ministeries, neem hier de tijd voor! Mogelijk willen M/R ook nog inzage vooraf.

Uitzonderingsgronden – Artikelen 10 en 11 Wob

Artikel 10

1. Het verstrekken van informatie ingevolge deze wet blijft achterwege voor zover dit:
 - a. de eenheid van de Kroon in gevaar zou kunnen brengen;
 - b. de veiligheid van de Staat zou kunnen schaden;
 - c. bedrijfs- en fabricagegegevens betreft, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
 - d. persoonsgegevens betreft als bedoeld in paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.
2. Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:
 - a. de betrekkingen van Nederland met andere staten en met internationale organisaties;
 - b. de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen;
 - c. de opsporing en vervolging van strafbare feiten;
 - d. inspectie, controle en toezicht door bestuursorganen;
 - e. de eerbiediging van de persoonlijke levenssfeer;
 - f. het belang, dat de geadresseerde erbij heeft als eerste kennis te kunnen nemen van de informatie;
 - g. het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.
3. Het tweede lid, aanhef en onder e, is niet van toepassing voorzover de betrokken persoon heeft ingestemd met openbaarmaking.
4. Het eerste lid, aanhef en onder c en d, het tweede lid, aanhef en onder e, en het zevende lid, aanhef en onder a, zijn niet van toepassing voorzover het milieu-informatie betreft die betrekking heeft op emissies in het milieu. Voorts blijft in afwijking van het eerste lid, aanhef en onder c, het verstrekken van milieu-informatie uitsluitend achterwege voorzover het belang van openbaarmaking niet opweegt tegen het daar genoemde belang.
5. Het tweede lid, aanhef en onder b, is van toepassing op het verstrekken van milieu-informatie voor zover deze handelingen betreft met een vertrouwelijk karakter.
6. Het tweede lid, aanhef en onder g, is niet van toepassing op het verstrekken van milieu-informatie.

7. Het verstrekken van milieu-informatie ingevolge deze wet blijft eveneens achterwege voorzover het belang daarvan niet opweegt tegen de volgende belangen:

- a. de bescherming van het milieu waarop deze informatie betrekking heeft;
- b. de beveiliging van bedrijven en het voorkomen van sabotage.

8. Voorzover het vierde lid, eerste volzin, niet van toepassing is, wordt bij het toepassen van het eerste, tweede en zevende lid op milieu-informatie in aanmerking genomen of deze informatie betrekking heeft op emissies in het milieu.

Artikel 11

1. In geval van een verzoek om informatie uit documenten, opgesteld ten behoeve van intern beraad, wordt geen informatie verstrekt over daarin opgenomen persoonlijke beleidsopvattingen.

2. Over persoonlijke beleidsopvattingen kan met het oog op een goede en democratische bestuursvoering informatie worden verstrekt in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.

3. Met betrekking tot adviezen van een ambtelijke of gemengd samengestelde adviescommissie kan het verstrekken van informatie over de daarin opgenomen persoonlijke beleidsopvattingen plaatsvinden, indien het voornemen daartoe door het bestuursorgaan dat het rechtstreeks aangaat aan de leden van de adviescommissie voor de aanvang van hun werkzaamheden kenbaar is gemaakt.

4. In afwijking van het eerste lid wordt bij milieu-informatie het belang van de bescherming van de persoonlijke beleidsopvattingen afgewogen tegen het belang van openbaarmaking. Informatie over persoonlijke beleidsopvattingen kan worden verstrekt in niet tot personen herleidbare vorm. Het tweede lid, tweede volzin, is van overeenkomstige toepassing.

Toelichting uitzonderingsgronden

Absolute uitzonderingsgronden

Vier absolute uitzonderingsgronden waarbij het verstrekken van informatie zonder meer achterwege moet blijven (artikel 10, eerste lid Wob):

- a. *De eenheid van de Kroon*
De eenheid van de Kroon komt in gevaar wanneer informatie wordt verstrekt over de inhoud van de contacten tussen de Koningin en een of meer bewindslieden. De eenheid van de Kroon strekt zich ook uit tot de Kroonprins. Voorbeeld: correspondentie tussen Minister en Koningin.
- b. *De veiligheid van de Staat*
Het verstrekken van informatie blijft achterwege als dit de veiligheid van de Staat zou kunnen schaden. Hier kan worden gedacht aan de interne veiligheid van de Staat (informatie van inlichtingendiensten) en ook aan de externe veiligheid (onderwerpen op het terrein van Defensie). Voorbeeld: militaire geheimen en informatie van inlichtingendiensten.
- c. *Bedrijfs- en fabricagegegevens*
Het bestaan van deze uitzonderingsgrond strekt tot bescherming van bedrijfs- en fabricagegegevens die door bedrijven (vertrouwelijk) aan de overheid zijn verstrekt, bijvoorbeeld om steun te verkrijgen, en inzage daarvan door derden inzicht zou geven in bedrijfsgeheimen en concurrentiegegevens. Er is alleen sprake van bedrijfs- en fabricagegegevens als men uit die gegevens iets te weten kan komen over het productieproces, de afzet van producten of de kring van afnemers en leveranciers. Voorbeeld: offertes van verschillende bedrijven; tenderdocumenten.
- d. *Bijzondere persoonsgegevens*
Het verstrekken van informatie blijft eveneens achterwege als dit bijzondere gegevens in de zin van de Wet bescherming persoonsgegevens (de Wbp) betreft. De Wbp kent een apart openbaarheidsregime voor bijzondere persoonsgegevens. Dit zijn persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging, strafrechtelijke aangelegenheden en onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Alleen wanneer zonder meer duidelijk is dat verstrekking van dergelijke gegevens geen inbreuk maakt op de persoonlijke levenssfeer is het mogelijk informatie betreffende bijzonder persoonsgegevens te verstrekken. Voorbeeld: informatie over iemands geloof, levensovertuiging, ras.

Relatieve uitzonderingsgronden

Zeven relatieve uitzonderingsgronden waarbij een belangenafweging moet worden gemaakt tussen het bedoelde belang en het algemene belang bij openbaarheid (artikel 10, tweede lid van de Wob):

- a. *Betrekkingen met andere Staten en internationale organisaties*
Verstrekking mag achterwege blijven als de Nederlandse internationale betrekkingen schade oplopen door openbaarmaking van de informatie. Het is voldoende dat men voorziet dat het internationale contact (in het algemeen of in het bijzonder, bijvoorbeeld in het geval van internationale onderhandelingen) moeilijk/stroever zou gaan lopen door het verschaffen van de gevraagde informatie. Voorbeeld: stukken afkomstig van buitenlandse bewindspersonen, wanneer van de opsteller geen toestemming voor verstrekking is verkregen.
- b. *Economische of financiële belangen van de Staat*
Deze uitzonderingsgrond is van toepassing als de kans bestaat dat het verstrekken van de

gevraagde informatie leidt tot economisch of financieel nadeel voor de overheid. Voorbeeld: informatie die bij openbaarmaking de positie van de Staat in een onderhandeling zou verzwakken.

c. *Opsporing en vervolging van strafbare feiten*

Het belang van openbaarheid kan botsen met strafrechtelijke en opsporingsbelangen. Door deze uitzonderingsgrond kan worden voorkomen dat de opsporing en vervolging van strafbare feiten wordt gefrustreerd. Het moet daarbij gaan om gegevens die zijn verzameld door opsporingsambtenaren of het Openbaar Ministerie. Naast concrete strafzaken mag het ook gaan om meer algemene informatie over opsporings- en onderzoeksstrategieën. Voorbeeld: lijst met van bepaalde strafbare feiten verdachte personen.

d. *Inspectie, controle en toezicht*

Met een beroep op deze uitzonderingsgrond kan inzage worden geweigerd in documenten betreffende inspectie, controle en toezicht, bronnen, methoden en technieken van onderzoek etc. Inzage in deze stukken zou immers de vertrouwensrelatie tussen de overheid en de inspecteur, controller of toezichthouder ernstig kunnen verstoren. Ook zou het verstrekken van de informatie het onmogelijk kunnen maken om in de toekomst op een verantwoorde manier inspectie, controle of toezicht uit te oefenen. Ter bescherming van informanten en getuigen kan overigens ook een beroep worden gedaan op eerbiediging van de persoonlijke levenssfeer (zie hieronder). Voorbeeld: de bij het opstellen van asielambtsberichten gebruikte methoden en technieken.

e. *De eerbiediging van de persoonlijke levenssfeer*

Op basis van deze uitzonderingsgrond doet de overheid geen mededelingen aan derden over gegevens van persoonlijke aard. Deze grond is allereerst van toepassing op 'gewone' burgers (en informanten en getuigen), maar geldt in bepaalde gevallen ook voor bewindslieden, ambtenaren en bestuurders. Overigens kan door het invoeren van deze grond niet automatisch worden bereikt, dat niets hoeft te worden openbaar gemaakt/ gegeven; veelal moeten documenten wel worden gegeven, maar "geanonimiseerd", zodat de daarin opgenomen informatie niet tot personen herleidbaar is. Voorbeeld: namen en telefoonnummers van ambtenaren of derden.

f. *Het belang voor degene aan wie een document is gericht om dat als eerste in te zien*

Onder omstandigheden moet de geadresseerde van een besluit in staat worden gesteld om als eerste kennis te nemen van die informatie voordat deze aan anderen wordt bekendgemaakt. Deze grond kan leiden tot opschorten van de openbaarmaking totdat diegene het stuk heeft ontvangen of ingezien. Voorbeeld: besluit dat een bepaalde persoon aangaat, zoals een beslissing op bezwaar.

g. *Het voorkomen van onevenredige bevoordeling of benadeling van personen of instanties*

Deze grondslag is een restgrond, die bezwaren tegen openbaarmaking dekt, welke niet bestreken worden door de andere uitzonderingsgronden. Deze grond kan bijvoorbeeld worden ingeroepen als de gevraagde informatie nog in bewerking is, of als door openbaarmaking een onvolledig of onjuist beeld wordt geschapen, en verstrekking kan leiden tot onevenredige benadeling van betrokkenen (het bestuursorgaan, derden enz.). De ervaring leert dat de rechter zeer streng is over gebruik van deze rest-uitzonderingsgrond. Deze grond moet dus terughoudend worden toegepast.

Interne meningsvorming (persoonlijke beleidsopvatting in stukken voor intern beraad)

Uit documenten die zijn opgesteld ten behoeve van intern beraad wordt geen informatie verstrekt over de daarin neergelegde persoonlijke beleidsopvattingen (artikel 11 Wob).

Onder intern beraad wordt in de Wob verstaan: standpuntbepaling binnen één of meer bestuursorganen. Ook beraad met externe adviseurs kan onder omstandigheden 'intern' beraad zijn. Voorbeelden daarvan zijn de notulen van de Ministerraad, ambtelijke of politieke nota's en rapporten van ambtelijke commissies.

Onder persoonlijke beleidsopvatting wordt verstaan: een interne opvatting, voorstel, aanbeveling of conclusie van één of meer personen over een bestuurlijke aangelegenheid en de daartoe door hen aangevoerde argumenten. Wanneer het bestuursorgaan, dus de minister of iemand namens hem dat met het oog op de goede en democratische bestuursvoering noodzakelijk acht, kan over persoonlijke beleidsopvattingen eventueel toch informatie worden verstrekt, maar dat moet dan gebeuren in niet tot personen herleidbare vorm. Dit betekent dat de naam en functie van de betrokken personen weggelakt dienen te worden.

BZ-instructie digitaal lakken bij Wob-verzoeken

BZ gebruikt voor het digitaal lakken het programma 'Adobe Acrobat Pro DC'. U kunt dit programma aanvragen via SSC-ICT en bij de ICT servicebalie.

1. Lakken

U kunt een PDF-bestand lakken (passages onleesbaar maken = lakken) door gebruik te maken van de Redaction functie in Adobe Acrobat Pro. Let op: u dient al de onderstaande stappen te doorlopen om informatie volledig digitaal te verwijderen!

- Open een bestand met Adobe Acrobat Pro en klik in het scherm op Tools. Op het scherm verschijnen tabbladen.
- Klik onder 'Protect & Standardize' op het tabblad 'Redact'.
- Het tabblad bevat icoontjes die u achtereenvolgens dient te gebruiken bij het lakken:
 1. 'Mark for redaction': hiermee selecteert u een passage tekst die het programma vervolgens rood omlijnt. Herhaal dit voor de rest van het document.
 2. 'Apply Redactions': indien u zeker bent dat de gemarkeerde passages wegkunnen dan drukt u op Apply Redactions.
 3. 'Sanitize document': bent u klaar met het bewerken van het document dan dient u te drukken op Sanitize document. Hierdoor wordt alle verborgen informatie van het document verwijderd. U wordt vervolgens automatisch gevraagd het geschoonde document op te slaan. Let op: u dient dit te doen om de wijzigingen permanent te maken! Kies daarbij een andere naam dan het oorspronkelijke document: bijv. document x geredigeerd.

2. Toevoegen uitzonderingsgronden en/of tekst (optioneel)

Adobe Acrobat Pro kent daarnaast mogelijkheden om direct Wob-uitzonderingsgronden toe te voegen aan een gelakte passage.

a) Wob uitzonderingsgronden installeren

U dient daartoe eerst éénmalig het bestand Wob.xml te importeren. Dit bestand kunt u opvragen bij DJZ/NR.

- 1) Sla het bestand Wob.xml op onder 'My documents' op uw eigen schijf. Het bestand is te vinden onder HBBZ/juridische zaken/ wob-aanvragen;
- 2) Klik onder het tabblad 'Redact' op 'Properties';
- 3) Vink in het scherm dat hierna opent het vakje 'Use overlay tekst' aan;
- 4) Vink eveneens het vakje 'redaction code' aan;
- 5) Klik vervolgens op 'edit code';
- 6) Klik in het scherm dat opent op 'Import set';
- 7) Open vervolgens via het scherm dat verschijnt 'Wob_gronden_digitaal_lakken.xml' vanaf uw eigenschijf en druk op OK

b) Aanbrengen uitzonderingsgronden

U gaat nu te werk als onder 1, maar klikt na het rood omlijnen van een tekstdeel:

1. met uw rechter muisknop op het gemarkeerde vlak
2. in het popup-scherf dat verschijnt, treft u onderaan de tab Wob met daarin de uitzonderingsgronden
3. door te klikken op de gewenste uitzonderingsgrond wordt deze toegevoegd
4. u kunt op 1 gemarkeerde passage meerdere uitzonderingsgronden toevoegen door deze stappen te herhalen
5. een uitzonderingsgrond verwijderen kan door de grond in de lijst uit te klikken
6. na het drukken op 'Apply redactions' zal de tekst op de zwarte vlakken verschijnen en is wijzigingen niet meer mogelijk!

c) Overige mogelijkheden

- *Instellen standaard uitzonderingsgrond:* indien u steeds of veelvuldige dezelfde uitzonderingsgrond gebruikt, dan kunt u deze als standaard invoegen. Klik onder het tabblad 'Protections' op 'Redaction properties'. Vink in het Redaction Properties scherm 'Custom Tekst' aan en klik het vakje 'Redaction Code' aan. Klik onder 'Code Sets' Wob aan. Selecteer onder 'Code Entries' gewenste Wob uitzonderingsgrond en druk op 'Add Selected Entry'. Ga vervolgens over tot lakken conform procedure 1. In de gemarkeerde passages kunt u de uitzonderingsgronden wijzigen door er met de rechter muis knok op te klikken (zie procedure onder 2b).
- *Vrije tekst invoegen:* u kunt ook vrije tekst invoegen op de weglakte passages. Klik met de rechter muisknop op de gemarkeerde tekst en selecteer in het popup-scherf 'properties'. In het 'Redaction properties' dat verschijnt vinkt u 'Use overlay tekst' aan. Klik het vakje 'Custom tekst' aan en voer de gewenste tekst in. Ga vervolgens verder conform procedure 2. Wijzigingen van tekst gaat op dezelfde wijze.

3. Afronden

1. ***Vergeet niet na bewerking van een bestand af te sluiten met de 'Sanitize document' procedure.***
2. ***Tot nader order dient u de bewerkte bestanden uit te printen alvorens deze te verstrekken aan de verzoeker.***

Vragen: Neem contact op met DJZ/NR.



Bijlage 6

Handleiding Rubricering

Handleiding rubricering

Versie 1.3

maart 2015

1. Inleiding

1.1 Waarom deze handleiding?

Deze handleiding is een beknopte uitleg van het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) 2013 en is opgesteld voor alle medewerkers van de Rijkssoeverheid om te verhelderen wanneer en hoe bijzondere informatie te rubriceren en hoe om te gaan met deze informatie.

2. Het rubriceren van informatie

2.1 Wat is rubriceren en waarom wordt informatie gerubriceerd?

Rubriceren is het proces waarbij de opsteller van een document de mogelijke schade voor het departement, de Staat of haar bondgenoten, of de nationale veiligheid inschat in geval dat de informatie uitlekt, ongeautoriseerd wordt gewijzigd of niet meer beschikbaar is. Afhankelijk van deze mogelijke schade wordt het document een rubricering toegekend die overeenkomt met een geschikte set van beveiligingsmaatregelen. Iedereen die het document onder ogen krijgt dient op basis van de aangebrachte rubricering te weten welke beveiligingsmaatregelen moeten worden nageleefd.

Bij compartimentering is het niet primair het niveau van rubricering van een gegevensverzameling die de zwaarte van de rubricering van de compartimentering bepaalt, maar de afweging dat tot de bepaling van een TBB niveau moet leiden. Uit de afweging volgt een keuze voor het niveau van compartimentering. Het aanwezig zijn van gerubriceerde informatie is hierdoor één van de elementen die moet worden meegenomen in de TBB bepaling.

2.2 Welke niveaus van rubricering zijn er?

Er zijn vier rubriceringniveaus met elk een bijpassende set van beveiligingsmaatregelen:

- Departementaal VERTROUWELIJK (afgekort Dep. V.);
- Staatsgeheim CONFIDENTIEEL (afgekort Stg. C.);
- Staatsgeheim GEHEIM (afgekort Stg. G.);
- Staatsgeheim ZEER GEHEIM (afgekort Stg. ZG.).

2.3 Wie rubriceert en stelt deze vast?

De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering en rubriceringduur vast. In de praktijk is dit vaak degene die de eindparaaf plaatst.

2.4 Hoe wordt de rubricering bepaald?

De rubricering is gerelateerd aan de inhoud van de informatie waarbij rekening moet worden gehouden welke schade er wordt geleden als de informatie in handen komt van onbevoegden.

Centraal staat hierbij de vraag:

“Wat zijn de gevolgen als deze informatie in verkeerde handen komt?”

Deze vraag dient te worden gesteld om een afweging te kunnen maken hoe de informatie gerubriceerd moet worden. De tabel schadevorm/impact kan hierbij helpen.

In de impacttabel dient gekeken te worden welke schadevorm er kan optreden (verticaal) en welke impact dit kan hebben (horizontaal).

Tabel: Schadevorm/ impact

	Dep. VERTROUWELIJK	Stg. CONFIDENTIEEL	Stg. GEHEIM	Stg. ZEER GEHEIM
Impact	Schade aan de belangen van de ministerie (s)	Schade aan vitale belangen van de Staat of bondgenoten	Ernstige schade aan vitale belangen van de Staat of bondgenoten	Zeer ernstige schade aan vitale belangen van de Staat of bondgenoten
Schadevorm				
Politieke schade	Politieke schade aan een bewindspersoon	Aftreden bewindspersoon	Aftreden kabinet	Parlementaire crisis
Publiek vertrouwen	Verlies van publiek respect	Publieke verontwaardiging	Verlies aan vertrouwen	Structureel verlies aan vertrouwen
Diplomatieke schade	Te herstellen door ambtelijke opschaling	Te herstellen door politieke opschaling	Externe bemiddeling noodzakelijk	Lange termijn schade tov vrienden/oorlog
Financiële schade aan de economie, financiële schade voor ministeries of de Staat	> € 50 miljoen	> € 500 miljoen	> € 5 miljard	> € 50 miljard
Financiële schade door openbaarmaking, concurrentiegevoelige bedrijfsgegevens, misbruik van vertrouwelijke verstrekte bedrijfsinformatie	Altijd ten minste Dep. VERTROUWELIJK	> € 5 miljoen	> € 500 miljoen	>€ 5 miljard
Schade aan vitale processen voor de samenleving	Verlies van zekerheid van continuïteit	Tijdelijk verlies van continuïteit	Langdurig verlies van continuïteit	Blijvende uitval van het proces
Schade aan bedrijfskritische processen van de Rijksdienst	Tijdelijk verlies van continuïteit	Langdurig verlies van continuïteit	Blijvende uitval van het proces	
Schending van privacy, schade aan burgers	Privacy gevoelige informatie van personen	Privacy gevoelige informatie van publieke figuren	Privacy gevoelige informatie van personen en informatie van het Koninklijk huis	Informatie van het Koninklijk huis

2.5 Hoe wordt er gerubriceerd?

Op een document als geheel wordt de rubricering rechtsboven en rechtsonder op iedere bladzijde en op de eventuele omslag aangegeven. Dit wordt als volgt gedaan:

Dep. VERTROUWELIJK

Stg. CONFIDENTIEEL

Stg. GEHEIM

Stg. ZEER GEHEIM

Alle rubriceringen zijn onderstreept. Op de verwisselbare gegevensdragers wordt de hoogste rubricering op de gegevensdrager aangegeven.

2.6 Derubriceren: Hoe werkt dat?

Omdat de beveiliging van gerubriceerde informatie belastend is voor de bedrijfsvoering dient deze te worden herzien of beëindigd zodra de noodzaak van de beveiliging wijzigt of eindigt. Dit kan na een bepaalde periode of gebeurtenis zijn (bijvoorbeeld als de inval heeft plaatsgevonden hoeven datum, tijdstip en adres niet meer geheim gehouden te worden), danwel bij overbrenging naar een archiefbewaarpplaats.

De vaststeller van de inhoud van de informatie of zijn ambtsopvolger is bevoegd de rubricering te beëindigen c.q. te wijzigen. Daarnaast zijn de SG, de beveiligingsambtenaar of een daartoe aangewezen rubriceringsambtenaar bevoegd de rubricering te beëindigen c.q. te wijzigen

2.7 Naast rubriceren: wat is merking?

Het is mogelijk dat naast de rubricering informatie te voorzien van een merking. Merkingen staan echter los van de rubricering van de informatie. Een merking geeft een bepaalde wijze van behandelen van de informatie aan. Hierbij valt te denken aan "spoed", "medisch geheim", "persoonlijk", "personeelsvertrouwelijk", etc. De merking wordt linksboven, onderstreept en in kapitalen op elke pagina aangebracht.

2.8 Waar kan informatie worden verkregen?

Voor uitgebreide informatie kunt u terecht bij de Beveiligingsambtenaar (BVA) van uw departement.

3. Internationale afspraken

3.1 Hoe wordt er omgegaan met buitenlandse rubricering?

Voor NAVO en EU gerubriceerde informatie dient men zich primair te houden aan de NAVO-respectievelijk EU regels. Deze zijn beschikbaar op roadmap-cd's waar de BVA de beschikking over heeft. De buitenlandse rubricering blijft gehandhaafd en wordt niet vervangen door een Nederlandse rubricering. Belangrijke verschillen in de verwerking van gerubriceerde informatie van internationale herkomst zijn dat voor alle rubriceringniveaus rekening gehouden dient te worden met spionage en dat voordat het gebruikt mag worden naast de SG ook de NSA (dit is het NBV voor alle departementen m.u.v. Defensie) toestemming gegeven moet hebben. De BVA kan helpen met deze toestemmingsverlening. Gerubriceerde informatie van internationale herkomst is ook bijzonder in de zin dat openbaarmaking, beëindiging of herziening van de rubricering niet is toegestaan zonder voorafgaande schriftelijke goedkeuring van het land van herkomst.

3.2 Welke beveiligingsniveaus van rubricering zijn er vastgelegd in verdragen? .

De belangrijkste rubriceringen binnen de verdragen zijn:

Nederland	NAVO	EU
Dep. Vertrouwelijk	NATO RESTRICTED	RESTREINT UE/EU RESTRICTED
Staatsgeheim CONFIDENTIEEL	NATO CONFIDENTIAL	CONFIDENTIEL UE/EU CONFIDENTIAL
Staatsgeheim GEHEIM	NATO SECRET	SECRET UE/EU SECRET
Staatsgeheim ZEER GEHEIM	COSMIC TOP SECRET	TRÉS SECRET UE/EU TOP SECRET

4. Hoe om te gaan met gerubriceerde informatie?

4.1 Mag er een (digitale) kopie worden gemaakt?

Mag gerubriceerde informatie gekopieerd worden? Er wordt onderscheid gemaakt tussen de hoogte van de rubriceringen.

Dep. Vertrouwelijk	Stg. Confidentieel	Stg. Geheim	Stg. Zeer Geheim
Kopiëren toegestaan.	Er mogen niet meer kopieën van bijzondere informatie gemaakt dan strikt noodzakelijk .	Er mogen niet meer kopieën van bijzondere informatie gemaakt dan strikt noodzakelijk .	Er mogen niet meer kopieën van bijzondere informatie gemaakt dan strikt noodzakelijk

4.2 Mag gerubriceerde informatie via de e-mail worden verstuurd?

Indien gerubriceerde informatie digitaal gedeeld wordt gedeeld gelden er de volgende afspraken voor het delen via e-mail. Er wordt onderscheid gemaakt tussen de hoogte van de rubriceringen.

Dep. Vertrouwelijk	Stg. Confidentieel	Stg. Geheim	Stg. Zeer Geheim
Verzenden via e-mail binnen de Rijksoverheid is toegestaan bij veilige koppelingen; Verzenden over het Internet enkel toegestaan indien gebruik gemaakt wordt van geëvalueerde producten.	Verzenden via e-mail binnen de Rijksoverheid of over het Internet is uitsluitend toegestaan met goedgekeurde geëvalueerde crypto middelen	Verzenden via e-mail is uitsluitend toegestaan met goedgekeurde geëvalueerde crypto middelen.	Verzenden via e-mail is niet toegestaan.

4.3 Mag gerubriceerde informatie worden gefaxt?

Ook voor het delen van gerubriceerde informatie via de fax gelden afspraken. Ook hierbij wordt onderscheid gemaakt tussen de hoogte van de rubriceringen.

Dep. Vertrouwelijk	Stg. Confidentieel	Stg. Geheim	Stg. Zeer Geheim
Ja binnen de Rijksoverheid mag dat, zolang het om vertrouwde internet verbindingen gaat met goedgekeurde middelen. Zolang de ontvanger voor verzending	Ja met gebruik van een cryptofax	Ja met gebruik van een cryptofax	Ja met gebruik van een cryptofax

wordt geïnformeerd.			
---------------------	--	--	--

4.4 Hoe wordt gerubriceerde informatie per post verstuurd?

Wanneer gerubriceerde informatie verstuurd moet worden dienen daarbij onderstaande regels gehandhaafd te worden. Verzending van gerubriceerde informatie dient te allen tijde in een dubbele envelop en in een sealbag te gebeuren.

Rubricering		
Dep. Vertrouwelijk	Per post geadresseerd op de persoon is toegestaan.	Bij verspreiding wordt de informatie voorzien van: Rubriceringsniveau, -duur, bladzijdenummering en het totaal aantal bladzijden waaruit het document bestaat.
Stg. Confidentieel	Verzenden geschiedt door: a. een geautoriseerde medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens het transport (opening moet gedetecteerd kunnen worden); b. een door de beveiligingsambtenaar goedgekeurde koerier.	Bij verspreiding wordt de informatie voorzien van: Rubriceringsniveau, -duur, bladzijdenummering en het totaal aantal bladzijden waaruit het document bestaat. Elk document is voorzien van een exemplaarnummer
Stg. Geheim	Fysieke verzending geschiedt door: a. een geautoriseerde medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens het transport; b. een door de beveiligingsambtenaar goedgekeurde koerier.	Bij verspreiding wordt de informatie voorzien van: Rubriceringsniveau, -duur, bladzijdenummering en het totaal aantal bladzijden waaruit het document bestaat. Elk document is voorzien van een exemplaarnummer
Stg. Zeer Geheim	Een Stg. Zeer Geheim document mag uitsluitend persoonlijk in handen van de geadresseerde worden gesteld. Nationale verzending uitsluitend via een overheidskoerier. Internationale verzending uitsluitend als diplomatieke koerierszending of militair transport.	Bij verspreiding wordt de informatie voorzien van: Rubriceringsniveau, -duur, bladzijdenummering en het totaal aantal bladzijden waaruit het document bestaat. Elk document is voorzien van een exemplaarnummer

4.5 Hoe wordt gerubriceerde informatie fysiek vervoerd?

Het uitgangspunt voor het vervoeren en verzenden van bijzondere informatie is dat de beveiliging van transport gehandhaafd blijft. Daarbij is van belang dat de transporteur geen inzage mag hebben in de informatie. Om dit te bereiken dient de bijzondere informatie deugdelijk verpakt te worden. Anders dan bij vervoeren, heeft de transporteur bij het meenemen wel inzage in de informatie. Het betreft hier vaak de informatie-eigenaar.

Voor het meenemen van bijzondere informatie buiten de locatie gelden andere, aanvullende regels. Hieronder wordt verstaan het meenemen naar een andere locatie, zoals de werkplek thuis en andere locaties die niet binnen het gecontroleerde gebied vallen (i.c. alle locaties waar de beveiliging niet onder het directe beheer van het departement valt). Voor de duidelijkheid zij vermeld dat het lijnmanagement een uiterst terughoudend beleid dient te voeren inzage het buiten e beveiligde werkomgeving brengen van bijzondere informatie.

Toestemming wordt uitsluitend verleend na een afweging van het bedrijfsbelang tegen de risico's van schending van de exclusiviteit van de gegevens. Indien de noodzaak is vastgesteld worden passende maatregelen getroffen om deze risico's te beperken en tot een acceptabel niveau terug te brengen. Ten aanzien van het thuis elektronisch verwerken van bijzondere informatie (zgn. telewerken) geldt als regel dat dit alleen is toegestaan middels de beveiligde telewerkdienst van het departement en dan alleen nadat toestemming van de lijnmanager is verkregen. De telewerkvoorziening is niet zonder meer geschikt voor e verwerking van gerubriceerde informatie. Voordat gebruik wordt toegestaan dienen aanvullende beveiligingsmaatregelen te worden getroffen. De lijnmanager overlegt dit vooraf met de BVA.

Rubricering	VIR-BI eisen verpakken, vervoeren en verzenden
Stg. ZG	<p><u>Verpakken, vervoeren en verzenden</u></p> <ul style="list-style-type: none"> • Verzending alleen per aangewezen koerier met ontvangstbevestiging • Verzending in dubbele enveloppe, het ontvangstbewijs wordt in de binnenenveloppe ingesloten • Rubricering wordt vermeld op de binnenenveloppe • Binnenenveloppe kan niet worden geopend zonder verbreking van de sluiting of beschadiging van de enveloppe • Verzender ziet toe op terugontvangst ontvangstbewijs • Geen elektronische verzending <p><u>Meenemen buiten de locatie</u></p> <ul style="list-style-type: none"> • Uitsluitend buiten gecontroleerd gebied brengen indien dit voor de voortgang van de werkzaamheden noodzakelijk is en er door de lijnmanager toestemming voor is verleend • Informatie met deze rubricering wordt niet mee naar huis genomen (zowel in fysieke vorm als elektronisch)
Stg. G	<p><u>Verpakken, vervoeren en verzenden</u></p> <ul style="list-style-type: none"> • Verzending alleen per aangewezen koerier met ontvangstbevestiging, indien dit niet mogelijk is per aangetekende post met ontvangstbevestiging • Verzending in dubbele enveloppe, het ontvangstbewijs wordt in de binnenenveloppe gesloten • Rubricering wordt vermeld op de binnenenveloppe • Binnenenveloppe kan niet worden geopend zonder verbreking van de sluiting of beschadiging van de enveloppe • Verzender ziet toe op terugontvangst ontvangstbewijs • Elektronisch vervoer/verzenden: informatie wordt gecijferd <p><u>Meenemen buiten de locatie</u></p> <ul style="list-style-type: none"> • Uitsluitend buiten gecontroleerd gebied brengen indien dit voor de voortgang van de werkzaamheden noodzakelijk is en er door de lijnmanager toestemming voor is verleend
Stg. C	<p><u>Verpakken, vervoeren en verzenden</u></p> <ul style="list-style-type: none"> • Verzending per aangetekende post of door goedgekeurde commerciële koerier • Verzending in dubbele enveloppe • Rubricering wordt vermeld op de binnenenveloppe • Elektronisch vervoer/verzenden: informatie wordt gecijferd <p><u>Meenemen buiten de locatie</u></p> <ul style="list-style-type: none"> • Uitsluitend buiten gecontroleerd gebied brengen indien dit voor de voortgang van de werkzaamheden noodzakelijk is en er door de lijnmanager toestemming voor is verleend

Dep. V	<u>Verpakken, vervoeren en verzenden</u> <ul style="list-style-type: none"> Elektronisch vervoer/ verzenden: informatie wordt versleuteld <u>Meenemen buiten de locatie</u> <ul style="list-style-type: none"> Uitsluitend buiten gecontroleerd gebied brengen indien dit voor de voortgang van de werkzaamheden noodzakelijk is en er door de lijnmanager toestemming voor is verleend

4.6 Hoe wordt gerubriceerde informatie bewaard?

Ook voor het bewaren van gerubriceerde informatie gelden afspraken. Daarbij moet altijd eerst besloten worden of het noodzakelijk is om de informatie te bewaren.

Voor het normenkader beveiliging rijksgebouwen wordt verwezen naar het normenkader dat in 2011 is vastgesteld.

4.7 Het bewaren van fysieke documenten of informatiedragers

Dep. Vertrouwelijk	Bewaren in een afgesloten en goedgekeurd opbergmiddel.
Stg. Confidentieel	Bewaren uitsluitend in een goedgekeurde kluis in een ruimte met inbraakalarmering.
Stg. Geheim	Bewaren uitsluitend in een goedgekeurde kluis in een ruimte met bewegingsdetectie, waarbij de weerstandstijd van de kluis groter is dan de interventietijd van de beveiliging.
Stg. Zeer Geheim	Bewaren uitsluitend in een goedgekeurde kluis in een ruimte met bewegingsdetectie, waarbij de weerstandstijd van de kluis groter is dan de interventietijd van de beveiliging.

4.8 Het bewaren van digitale informatie

Dep. Vertrouwelijk	Bewaren op een afgeschermd deel van de netwerkopslag of op een beveiligde USB-stick.
Stg. Confidentieel	Bewaren uitsluitend op een goedgekeurde USB-stick, na gebruik opgeborgen in een goedgekeurde kluis.
Stg. Geheim	Op een DWR-G werkplek?
Stg. Zeer Geheim	

4.9 Vernietigen: mag dat?

Ook gerubriceerde informatie dient op grond van de Aarchiefwet 1995 (op termijn) te worden vernietigd dan wel worden overgedragen aan een archiefbewaarplaats. Welke stukken vernietigd moeten worden, is vastgelegd in zgn. selectielijsten. Van de daadwerkelijke vernietiging wordt een verklaring van vernietiging opgesteld. De beveiligingsambtenaar kan aanvullende eisen stellen aan de wijze van vernietiging.



Bijlage 7

VIRBI 2013



Besluit van de Minister-President, Minister van Algemene Zaken van 1 juni 2013, nr. 3124134, houdende voorschrift informatiebeveiliging Rijksdienst – bijzondere informatie 2013

De Minister-President, Minister van Algemene Zaken,

Handelend in overeenstemming met het gevoelen van de ministerraad,

Besluit:

Artikel 1 Begripsbepalingen

In dit besluit wordt verstaan onder:

- a. *Bijzondere informatie*: informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries;
- b. *Compromittering*: kennisname dan wel mogelijkheid tot kennisname van bijzondere informatie door niet geautoriseerden;
- c. *Rubriceren*: bepalen van het rubriceringsniveau en -duur van de bijzondere informatie op basis van de te verwachten nadelige gevolgen voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) deze informatie bekend wordt bij niet geautoriseerden;
- d. *Rubriceringsniveau*: aanduiding van de verwachte nadelige gevolgen aan de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) de informatie bekend wordt bij niet geautoriseerden;
- e. *Rubriceringsambtenaar*: ambtenaar bevoegd tot het vaststellen van rubriceringen, hiertoe aangewezen door de secretaris-generaal;
- f. *Vaststeller van de rubricering*: minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal aangewezen rubriceringsambtenaar;
- g. *Rijksdienst*: alle organisatieonderdelen waarvoor de ministeriële verantwoordelijkheid onverkort geldt.
- h. *Zorgdrager*: degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

Artikel 2 Plaatsbepaling en reikwijdte

1. Dit voorschrift met de bijbehorende toelichting en bijlage 1 geldt voor de Rijksdienst, waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.
2. Op de beveiliging van bijzondere informatie zijn de bepalingen van dit voorschrift als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013) van toepassing.
3. Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen, behoudt de toegekende rubricering en wordt beveiligd volgens het overeenkomstige nationale beveiligingsniveau. Voor zover voor de beveiliging van dergelijke informatie als gevolg van het verdrag of de overeenkomst afwijkende of verdergaande beveiligingsbepalingen bestaan worden deze bepalingen toegepast.

Artikel 3 Beveiligingsbeleid

Het beveiligingsbeleid dat door de secretaris-generaal wordt vastgesteld omvat ten minste de ministeriële uitgangspunten voor de beveiliging van, de toegang tot, het omgaan met en verwerken van bijzondere informatie zoals bedoeld in dit voorschrift en de wijze waarop:

- a. het ministerie informatie rubriceert;
- b. de secretaris-generaal vooraf toestemming verleent voor het verwerken van bijzondere informatie;
- c. het ministerie toezicht uitoefent op de beveiliging van bijzondere informatie.

Artikel 4 Rubriceringen

1. Informatie waarvan de geheimhouding vanwege het belang van de Staat, zijn bondgenoten of van één of meer ministeries is geboden, moet worden voorzien van een passend niveau van rubricering.



2. Bijzondere informatie wordt als volgt gerubriceerd:
 - a. Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG)
Indien kennisname door niet geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
 - b. Staatsgeheim GEHEIM (afgekort Stg.G)
Indien kennisname door niet geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
 - c. Staatsgeheim CONFIDENTIEEL (afgekort Stg.C)
Indien kennisname door niet geautoriseerden schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
 - d. Departementaal VERTROUWELIJK (afgekort Dep.V.).
Indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.
3. De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.

Artikel 5 Herzien en beëindigen van de rubricering

1. Rubriceringen worden verbonden aan een maximum tijdsverloop of aan een bepaalde gebeurtenis. Na die periode of na die gebeurtenis weegt de vaststeller voor bijzondere informatie af of herziening, dan wel beëindiging van de rubricering, aan de orde is.
2. Van het eerste lid van deze bepaling kan worden afgeweken in die gevallen waarin de rubricering betrekking heeft op:
 - a. Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen;
 - b. Staatsgeheimen die door de wet als zodanig zijn aangewezen.
3. Uitsluitend de vaststeller van de rubricering is bevoegd de rubricering te herzien of te beëindigen.
4. Bij overbrenging van bijzondere informatie naar een rijksarchiefbewaarplaats als bedoeld in de Archiefwet 1995 vervalt de rubricering, tenzij de zorgdrager, na advies van de algemene rijksarchivaris, bepaalt dat deze gehandhaafd dan wel herzien moet worden.

Artikel 6 Eisen aan de beveiliging

1. Bijzondere informatie wordt zodanig beveiligd dat:
 - a. alleen personen die daartoe zijn geautoriseerd deze kunnen behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak en
 - b. dat inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is.
2. De beveiliging is ingericht op basis van risicomanagement.
3. Bijzondere informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen wordt uitsluitend verwerkt nadat de autoriteit, die krachtens het betreffende verdrag verantwoordelijk is voor de beveiligingsregels ter bescherming van bijzondere informatie, haar goedkeuring aan de beveiliging heeft gegeven.

Artikel 7 Buiten de rijkdienst brengen van bijzondere informatie

1. Bij het buiten de rijkdienst brengen van bijzondere informatie, anders dan op grond van een wettelijke verplichting tot openbaarmaking, blijven de eisen aan de beveiliging en het toezicht daarop onverkort van kracht.
2. Bijzondere informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen wordt uitsluitend na voorafgaande toestemming van het land of de internationale organisatie van herkomst doorgegeven aan externe partijen.

Artikel 8 Compromittering van bijzondere informatie

1. Elke ambtenaar is verplicht de Beveiligingsambtenaar (BVA) onmiddellijk mededeling te doen van een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van bijzondere informatie.
2. De BVA laat, nadat hij op de hoogte is gebracht van een inbreuk op de beveiliging, onmiddellijk



(nood)maatregelen treffen om verdere inbreuk te voorkomen.

3. De BVA onderzoekt of compromittering van bijzondere informatie heeft plaatsgevonden; indien dit het geval is doet hij hiervan mededeling aan de secretaris-generaal en adviseert over de noodzaak tot het instellen van een commissie van onderzoek.
4. Indien de compromittering betrekking heeft op bijzondere informatie die is verkregen van een ander ministerie of krachtens internationaal verdrag of overeenkomst, doet de BVA bovendien mededeling aan dat betreffende ministerie of de krachtens het verdrag of de overeenkomst voor de beveiliging van die bijzondere informatie verantwoordelijke instantie.

Artikel 9 Commissie van onderzoek

1. Een commissie van onderzoek wordt ingesteld door de secretaris-generaal.
2. De commissie stelt een onderzoek in naar:
 - a. de wijze waarop de compromittering heeft plaatsgevonden;
 - b. de aard en de omvang van de schade aan de belangen van de Staat of zijn bondgenoten;
 - c. de te nemen maatregelen om de schade te beperken en herhaling te voorkomen.
3. De commissie voert, indien de gecompromitteerde bijzondere informatie (mede) afkomstig is van een ander ministerie, haar onderzoek uit in overleg met de BVA van dat ministerie. In het geval dat de gecompromitteerde bijzondere informatie krachtens een internationaal verdrag of overeenkomst is verkregen voert de commissie haar onderzoek uit in samenwerking met de instantie die krachtens het verdrag of de overeenkomst verantwoordelijk is voor de beveiliging ervan.
4. De secretaris-generaal of een door hem aangewezen ambtenaar treft, op basis van de bevindingen van de commissie van onderzoek, maatregelen om de schade die de compromittering heeft toegebracht aan de veiligheid of andere gewichtige belangen van de Staat of zijn bondgenoten te beperken en herhaling van de compromittering te voorkomen.
5. Indien het de compromittering van een staatsgeheim betreft stelt de secretaris-generaal het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst in kennis van de uitkomsten van het onderzoek. Bij het ministerie van Defensie wordt de Militaire Inlichtingen- en Veiligheidsdienst op de hoogte gesteld van de uitkomsten van het onderzoek.

Artikel 10 Slotbepaling

1. Het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie van 24 februari 2004 wordt ingetrokken.
2. Rubriceringen die zijn vastgesteld vóór inwerkingtreding van dit voorschrift worden uiterlijk tien jaar na vaststelling door de vaststeller onderzocht op de mogelijkheid om de rubricering te herzien of te beëindigen.
3. Dit besluit en de daarbij behorende bijlagen treden in werking met ingang van 1 juni 2013.
4. Dit besluit wordt aangehaald als: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).
5. Dit besluit zal met de toelichting in de Staatscourant worden geplaatst. Van de ter inzage legging van de bij dit besluit behorende bijlagen zal mededeling worden gedaan in de Staatscourant.

*De Minister-President, Minister van Algemene Zaken,
M. Rutte.*



BIJLAGE 1. UITGANGSPUNTEN EN MINIMUM NIVEAU BEVEILIGING

Deze bijlage beschrijft de uitgangspunten en het minimum beveiligingsniveau voor de beveiliging van bijzondere informatie. Bij de inrichting van een adequaat stelsel van beveiligingsmaatregelen voor de beveiliging van bijzondere informatie moet binnen het in de artikelen beschreven principe van risicomangement worden uitgegaan van de volgende inrichtingsprincipes:

- Beveiliging in lagen: De beveiliging zal bestaan uit meerdere lagen, zodat er geen afhankelijkheid is van één beveiligingsmaatregel.
- Minste privilege: Alleen de autorisaties die iemand nodig heeft om zijn taak te kunnen vervullen, zullen worden toegekend;
- Zelf beschermende systemen: Ieder systeem beschouwt andere systemen als onvertrouwd totdat het tegendeel is bewezen en treft maatregelen om veilig informatie uit te kunnen wisselen met wel vertrouwde systemen indien deze communicatie via onvertrouwde systemen verloopt.
- Verificatie implementatie beveiliging: De maatregelen voor beveiliging van bijzondere informatie worden onder de verantwoordelijkheid van de BVA of de accreditatieautoriteit periodiek gecontroleerd.

Deze inrichtingsprincipes moeten stringenter worden toegepast naarmate het niveau van de rubricering toeneemt.

Voor de volgende onderwerpen, die grotendeels afkomstig zijn uit de Code voor Informatiebeveiliging, zijn specifiek op bijzondere informatie toegesneden doelstellingen en eisen geformuleerd waaraan dient te worden voldaan. Waar aan de orde zijn daarbij ook maatregelen benoemd die ten minste deel uit moeten maken van de totale set van maatregelen om de vertrouwelijkheid van bijzondere informatie te waarborgen.

Hiermee is voor alle betrokkenen inzichtelijk gemaakt wat minimaal wordt verlangd op het gebied van beveiliging voor de verschillende rubriceringen op grond van dit voorschrift. Tevens is op efficiënte wijze de toepassing van een uniforme set van minimale maatregelen gedefinieerd waardoor waarborgen zijn gecreëerd voor een consistente beveiliging van bijzondere informatie.

1. Management van bedrijfsmiddelen

Doelstelling

Het handhaven van een adequaat, ordelijk en controleerbaar beheer van bedrijfsmiddelen waarop bijzondere informatie wordt verwerkt.

Eis

Bedrijfsmiddelen waarop bijzondere informatie wordt verwerkt, dienen te zijn geregistreerd en aan een 'eigenaar' te zijn toegewezen. Daarbij is onderkend welke van deze bedrijfsmiddelen specifieke beveiligingsmaatregelen behoeven.

	Dep.V	Stg.C	Stg.G	Stg.ZG
A Maatregel Registreer alle middelen en de personen aan wie deze zijn uitgereikt.			V	V
B Maatregel Registreer de locatie/standplaats van alle middelen en de toewijzing aan een eigenaar.			V	V

2. Personen

Doelstelling

Organisaties moeten zekerstellen dat personen hun verantwoordelijkheden kennen en geschikt zijn voor de rol die zij vervullen evenals het beperken van de risico's van menselijk handelen.

Eis

Elk persoon die frequent gaat werken met bijzondere informatie, dient voorafgaand aan indiensttreding een aan zijn functie vervulling gerelateerd betrouwbaarheidsonderzoek te ondergaan. Voor het bepalen of een functie als vertrouwensfunctie moet worden aangewezen, dient de betreffende leidraad aanwijzen vertrouwensfuncties van de AIVD (civiele sector) en MIVD (militaire sector) te worden gevolgd.

Bij beëindiging of wijziging van het dienstverband waarin gewerkt is met bijzondere informatie, wordt zeker gesteld dat de geheimhoudingsplicht geborgd is.

Van elk persoon die frequent werkt met bijzondere informatie moet geborgd zijn dat deze over een aan zijn functie vervulling gerelateerd, actueel betrouwbaarheidsonderzoek beschikt.

	Dep.V	Stg.C	Stg.G	Stg.ZG
A Maatregel Personen die hebben te maken met bijzondere informatie, dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	V	V	V	V
B Maatregel Personen die frequent hebben te maken met bijzondere informatie dienen tevens te beschikken over een passende verklaring.	VOG ¹	VGB ²	VGB ²	VGB ²
C Maatregel Bij beëindiging van een functie waarbij iemand in aanraking komt met bijzondere informatie wordt zeker gesteld dat de betreffende persoon geen toegang meer heeft tot die informatie, noch deze in zijn / haar bezit heeft.	V	V	V	V

¹ Verklaring omtrent het gedrag

² Verklaring van geen bezwaar conform de Wet op de veiligheidsonderzoeken

3. Fysieke en omgevingsbeveiliging

Doelstelling

Het waarborgen van toereikende weerstand tegen (pogingen tot) ongeautoriseerde fysieke toegang van locaties, gebouwen en ruimtes (waaronder kluizen) waar zich bijzondere informatie bevindt.

Eis

Voor elke locatie, gebouw en ruimte waar zich bijzondere informatie bevindt, dient systematisch de beveiligingsmaatregelen in beeld te zijn gebracht voor fysieke toegangsbeheersing. Hierbij is ten minste voorzien in:

- Het aanbrengen van zonering c.q. compartimentering.
- Het detecteren van ongeautoriseerde toegangen of pogingen daartoe.
- Het regelen van een ordelijk toegangsbeleid en sleutelbeheer.
- Het uitoefenen door bewakingspersoneel van toezicht buiten reguliere werktijden.
- Het toewijzen van ruimten waar met bijzondere informatie mag worden gewerkt.

Ten aanzien van zonering kunnen de diverse beveiligingszones worden onderkend, waarbij om toegang te krijgen tot ruimtes waarin bijzondere informatie wordt verwerkt, steeds zwaardere beveiligingsmaatregelen worden getroffen.

	Dep.V	Stg.C	Stg.G	Stg.ZG
A Maatregel Bijzondere informatie wordt zodanig behandeld en opgeslagen dat er een positief beveiligingsrendement ¹ is, op basis van schadeacceptatie en het dreigingsprofiel.	V	V	V	V
B Maatregel Tempestmaatregelen conform Beleidsadvies Compromitterende straling (VBV 32000).		V	V	V
C Maatregel Tegengaan van af luisteren, zicht op en reflectie van informatie (bv via beeldschermen of spiegelende oppervlakten).		V	V	V
D Maatregel De medewerker verantwoordelijk voor de verwerking van bijzondere informatie, dient zorg te dragen dat bezoekers geen kennis kunnen nemen van de bijzondere informatie die hij onder zijn beheer heeft.	V	V	V	V
E Maatregel Bezoekers worden begeleid wanneer zij ruimten waarin bijzondere informatie aanwezig is, betreden.		V	V	V
F Maatregel Bezoekers worden geregistreerd indien zij toegang (kunnen) hebben tot bijzondere informatie in ruimten die zij betreden, als de toegang tot die informatie niet op andere wijze kan worden voorkomen (bv kast/kluizen/etc.).			V	V

¹ Zie hiervoor toelichting artikel 3 onder b.

4. Logische toegangsbeveiliging

Doelstelling

Het waarborgen van een beheerste en gecontroleerde toegang tot ICT-voorzieningen waarin zich bijzondere informatie bevindt.

Eisen

Voorzie in procedures en regels voor toegangsrechten tot en monitoring van netwerkdiensten, besturingssystemen en applicaties waar zich gerubriceerde informatie bevindt.

Voorzie in een stelsel van logische toegangsbeveiligingsmaatregelen dat is gerelateerd aan de relevante dreiging en het rubriceringniveau.

	Dep.V	Stg.C	Stg.G	Stg.ZG
A <u>Maatregel</u> Toegang tot een account wordt na een aantal direct achtereenvolgende foutieve inlogpogingen geblokkeerd.	5	3	3	3
B <u>Maatregel</u> Toegang tot systemen kan op groepsniveau worden bepaald.	V	V	V	niet toegestaan
C <u>Maatregel</u> Toegang tot bijzondere informatie wordt op individueel niveau bepaald.			V	V

5. Levenscyclus ICT-voorzieningen

Doelstelling

Het waarborgen van een passend niveau van beveiliging gedurende de gehele levenscyclus van ICT-voorzieningen waarin bijzondere informatie wordt verwerkt.

Eis

Voorafgaand aan verwerving, ontwikkeling, onderhoud en afstoot van informatiesystemen waarin bijzondere informatie wordt verwerkt, dienen de dreigingen en risico's in beeld te zijn gebracht.

	Dep.V	Stg.C	Stg.G	Stg.ZG
A <u>Maatregel</u> Gedurende de gehele levenscyclus van een systeem worden periodieke audits, inspecties, reviews en tests uitgevoerd om te controleren of de beveiligingsmaatregelen effectief zijn. Deze controles worden uitgevoerd door deskundige specialisten die beschikken over de juiste onderzoeksmiddelen en beproefde onderzoeksmethoden.	Self assessment	Self assessment	Onafhankelijke deskundige	Onafhankelijke deskundige
B <u>Maatregel</u> De verantwoordelijkheden en procedures voor het adequaat beheer en juist gebruik van de ICT-voorzieningen waarin bijzondere informatie wordt verwerkt, zijn vastgesteld.	V	V	V	V
C <u>Maatregel</u> Voor het beheer van ICT-voorzieningen is het beveiligingsniveau in overeenstemming met de risico's.	V	V	V	V
D <u>Maatregel</u> Bij uitbesteding van (delen van) de dienstverlening dient een zelfde beveiligingsniveau te worden gerealiseerd als geldt bij de interne dienstverlening.	V	V	V	V

6. Verzending van gerubriceerde informatie

Doelstelling

Het waarborgen van een wederzijds verenigbaar beveiligingsniveau voor de vertrouwelijkheid van bijzondere informatie.



Eisen

Er dient te zijn voorzien in een passende set van verenigbare maatregelen indien bijzondere informatie het ministerie verlaat.

De vertrouwelijkheid van informatie moet tijdens (elektronisch) transport buiten gecontroleerd gebied gehandhaafd blijven

	Dep.V	Stg.C	Stg.G	Stg.ZG
A <u>Maatregel</u> Digitale verzending van bijzondere informatie dient met ministerieel goedgekeurde cryptografische middelen te geschieden. De ministeriële goedkeuring vindt plaats op basis van advies van de Werkgroep Bijzondere Informatiebeveiliging (WBI) of diens rechtsopvolger over de beveiligingswaarde van de cryptografische middelen.		V	V	V
B <u>Maatregel</u> Digitale verzending van informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen, dient met door de verstreckende instantie goedgekeurde cryptografische middelen te worden verzonden.			V	V
C <u>Maatregel</u> Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	V	V	V	V
D <u>Maatregel</u> Fysieke verzending geschiedt door: • een geautoriseerde medewerker, waarbij de informatie te allen tijde onder beheer van de drager blijft en niet wordt geopend tijdens transport • fysieke verzending geschiedt met een ministerieel goedgekeurde koerier. • een militaire, overheids- of diplomatieke koerier.		V	V	nvt
E <u>Maatregel</u> Nationale verzending uitsluitend via een overheidskoerier.				V
F <u>Maatregel</u> Internationale verzending uitsluitend als diplomatieke koeringszending of militair transport.				V
G <u>Maatregel</u> Zowel digitaal als niet digitaal is er een onweerlegbare bevestiging van ontvangst.		V	V	V
H <u>Maatregel</u> Beveiligingsrelevante handelingen worden geregistreerd.	V	V	V	V
I <u>Maatregel</u> Het maken, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling en vernietigen van bijzondere informatie wordt vastgelegd.			V	V
J <u>Maatregel</u> Elk document moet tenminste bij verspreiding voorzien zijn van: • Rubriceringsniveau; • Rubriceringsduur; • Bladzijdenummering en totaal aantal bladzijden waaruit het document bestaat;	V	V	V	V
K <u>Maatregel</u> Elk document wordt voorzien van: • Exemplaarnummer.		V	V	V
L <u>Maatregel</u> Van alle exemplaren van bijzondere documenten worden de volgende gegevens vastgelegd: • Exemplaarnummer; • Maker; • Ontvanger.		V	V	V
M <u>Maatregel</u> Er worden niet meer kopieën van bijzondere informatie gemaakt dan strikt noodzakelijk.		V	V	V



TOELICHTING OP DE ARTIKELEN VIRBI 2013

Artikel 1 Begripsbepalingen

Onder a:

Dit voorschrift gebruikt de term informatie onafhankelijk van het gebruikte medium en onafhankelijk of de informatie is vastgesteld. Het voorschrift betreft dus informatie in ruste (bijvoorbeeld opgenomen in documenten of databases), in bewerking (bijvoorbeeld in het geheugen van een computer) of in communicatie (telefoongesprekken, vergaderingen, datacommunicatie, andere elektromagnetische signalen).

Kennisname van bijzondere informatie dient beperkt te blijven tot geautoriseerde personen. Autorisatie vraagt om een expliciete en aantoonbare toestemming, waarbij de eisen aan de autorisatieprocedure met het rubriceringsniveau toenemen. Het is bij het verlenen van autorisatie niet voldoende dat een beoogde ontvanger over een verklaring van geen bezwaar van het juiste niveau beschikt. Er dient een afzonderlijke afweging gemaakt te worden over de functionele noodzaak tot kennisname door de betrokken persoon.

Onder b:

In de toelichting op de artikelen 8 en 9 wordt nader ingegaan op compromittering.

Onder c:

Voordat aan informatie een rubricering en rubriceringsduur kan worden toegekend, worden eerst afwegingen gemaakt over de te voorzien nadelige gevolgen die met een redelijke kans op kunnen treden; dit is nader uitgewerkt in de toelichting op artikel 4. De betekenis van de rubriceringsduur is nader uitgewerkt in de toelichting bij artikel 5, lid 1.

Onder d:

Er bestaan vier rubriceringsniveaus. De rubriceringen verschillen in de ernst van de nadelige gevolgen die zijn voorzien bij ongeautoriseerde kennisname. De toelichting op artikel 4 gaat hier nader op in.

Onder e:

De secretaris-generaal kan rubriceringsambtenaren aanwijzen die namens hem de rubricering vast kunnen stellen. In de regel zijn dit de hogere lijnfunctionarissen, de BVA en zijn plaatsvervanger of andere inhoudelijk deskundigen.

Onder h:

Op grond van artikel 23, eerste lid van de Archiefwet 1995 dragen de ministers zorg voor de archiefbescheiden die niet zijn overgebracht naar een rijksarchiefbewaarplaats. Als zorgdrager heeft de minister de bevoegdheid bij overbrenging beperkingen aan de openbaarheid te stellen.

Artikel 2 Plaatsbepaling en reikwijdte

Lid 1:

De artikelen bevatten op hoofdlijnen de werkwijze voor de behandeling van bijzondere informatie en de wijze van rubriceren. De uitwerking heeft dezelfde zeggingskracht en geeft nadere aanwijzingen over de inrichting van de rubricering en de verwerking van bijzondere informatie.

Tot de Rijksdienst behoren alle organisatieonderdelen waarvoor de ministeriële verantwoordelijkheid onverkort geldt. Het VIRBI 2013 heeft geen directe werking buiten de Rijksdienst (publieke en private partijen), waaronder ook zelfstandige bestuursorganen. Het kan echter noodzakelijk zijn om bijzondere informatie buiten de Rijksdienst te brengen. Het voorschrift staat dit alleen toe als voldoende zekerheid bestaat dat de informatie in overeenstemming met dit voorschrift wordt beveiligd. Centraal staat hierbij het waarborgen van de vertrouwelijkheid middels proportionele maatregelen. In het ministeriële beveiligingsbeleid (artikel 3) dient dit verder te worden uitgewerkt. Regels voor het buiten de rijksdienst brengen van bijzondere informatie worden gegeven in artikel 7.

Lid 2:

Het VIRBI 2013 is het raamwerk in aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en BVR 2013. Het geeft de regels voor de Rijksdienst voor de beveiliging van bijzondere informatie.

Het VIR 2007 geeft de regels voor de informatiebeveiliging voor de Rijksdienst. Het is een raamwerkregeling in de zin dat de werkwijze om tot een verantwoorde beveiliging te komen bepaald is, zonder een minimaal beveiligingsniveau voor de Rijksdienst op te leggen. Het BVR 2013 geeft de regels voor de integrale beveiliging voor de Rijksdienst.



Waar het VIR betrekking heeft op de gehele beveiliging van informatiesystemen, is alleen de vertrouwelijkheid van informatie het onderwerp van het VIRBI 2013. Dit houdt in dat voor de bescherming van de integriteit en beschikbaarheid van de informatie in informatiesystemen afwegingen in overeenstemming met het VIR gemaakt moeten worden. Dit geldt ook voor de bescherming van de vertrouwelijkheid van informatie die niet is gerubriceerd.

Lid 3:

Bijzondere informatie van internationale herkomst behoudt zijn oorspronkelijke rubricering. Dit houdt in dat de oorspronkelijke rubricering niet vervangen mag worden door een Nederlandse rubricering. Op dergelijke bijzondere informatie is primair niet het VIR-BI, maar een internationaal verdrag van toepassing. In dergelijke verdragen is opgenomen dat, behoudens enkele uitzonderingen, de nationale regelgeving wordt gevolgd:

1. Het VIRBI 2013. Het ministerie draagt zelf zorg voor een afdoende beveiliging en verantwoording.
2. Het internationaal verdrag kan een aantal uitzonderingen geven. Deze komen neer op een uiterst beperkte ruimte voor risicomanagement en gescheiden verwerking van nationale en internationale bijzondere informatie.
3. Toestemming voor ontvangst, beheer, verwerking en verdere verspreiding van dergelijke informatie dient verkregen te worden van de Security Accreditation Authority (SAA). De Secretaris-generaal van het ministerie is de SAA voor civiele omgevingen en de beveiligingsautoriteit van het ministerie van Defensie voor defensieomgevingen. Deze zijn verantwoordelijk om voorafgaand aan een toestemmingverlening (accreditatie), te (laten) onderzoeken of de beveiliging van de informatie voor wat betreft de bescherming van de internationale belangen aan de vereisten voldoet. De National Security Authority (NSA), respectievelijk civiel en militair, voert de controle op de beveiliging uit en verzorgt de verdere afhandeling naar de internationale organisaties. Het ministerie blijft zelf verantwoordelijk voor een afdoende beveiliging van de nationale belangen (voor zowel beschikbaarheid, integriteit als de vertrouwelijkheid). De 'Information Assurance'-functies die door de EU en NATO worden onderscheiden, zijn en worden met het instellingsbesluit van de Werkgroep Bijzondere Informatiebeveiliging (WBI) of haar rechtsopvolger toegewezen (IA-autoriteit, Tempest-autoriteit, Crypto Approval-autoriteit en Cryptodistributie-autoriteit).

Met betrekking tot NAVO en EU informatie wordt de volgende vergelijkingstabel gehanteerd om tot het vergelijkbaar nationaal niveau te komen:

Nederlands	NAVO	EU
Dep. VERTROUWELIJK	NATO RESTRICTED	RESTREINT UE/EU RESTRICTED
Stg. CONFIDENTIEEL	NATO CONFIDENTIAL	CONFIDENTIEEL UE/EU CONFIDENTIEEL
Stg. GEHEIM	NATO SECRET	SECRET UE/EU SECRET
Stg. ZEER GEHEIM	COSMIC TOP SECRET	TRÈS SECRET UE/EU TOP SECRET

Met betrekking tot informatie die bilateraal uit andere landen wordt ontvangen, wordt dit conform de bilaterale overeenkomst behandeld. Indien er geen bilaterale overeenkomst is, kan middels de bovenstaande tabel een vergelijkbaar nationaal niveau bepaald worden voor de beveiliging, in afstemming met de eigenaar van de informatie.

Het kan noodzakelijk zijn om aan informatie gelijktijdig zowel nationale als internationale rubriceringen toe te kennen. Indien bijvoorbeeld documenten zijn samengesteld met informatie uit verschillende bronnen met verschillende rubriceringen dan behoudt de informatie iedere oorspronkelijke rubricering van de broninformatie.

Artikel 3 Beveiligingsbeleid

Dit artikel geeft met betrekking tot bijzondere informatie aanvullende bepalingen ten opzichte van de eisen die het VIR 2007 in artikel 3 aan het beveiligingsbeleid stelt. Het ministeriële beleid geeft de aanwijzingen voor de wijze waarop de medewerkers met bijzondere informatie omgaan; het VIRBI 2013 geeft de kaders voor dit ministerieel beleid.

Het VIRBI 2013 bevat, ten opzichte van het VIR 2007, drie aanvullende onderwerpen voor het beleid. De onderwerpen hebben betrekking op de wijze waarop het ministerie informatie rubriceert, de wijze waarop de secretaris-generaal vooraf toestemming verleent voor het verwerken van bijzondere informatie en de wijze waarop het ministerie toezicht uitoefent op de beveiliging van bijzondere informatie. De onderwerpen kunnen onderdeel uitmaken van een integraal beleidsdocument of afzonderlijk worden vastgelegd.

Onder a:

Dit omvat zowel de wijze waarop binnen het ministerie tot rubricering wordt besloten als de te hanteren criteria om tot de juiste rubricering te komen. Belangrijk is hierbij af te wegen dat naarmate het rubriceringsniveau van informatie hoger ligt, de beveiligingseisen toenemen, waarmee de beperkingen door en de kosten van de beveiliging ook navenant toe kunnen nemen.

Onder b:

Het belang dat met bijzondere informatie gemoeid is, maakt een expliciete afweging op centraal niveau noodzakelijk om reeds op voorhand te waarborgen dat de informatieverwerking zorgvuldig geschiedt. Daarom wordt in het beleid vastgelegd hoe vooraf toestemming wordt gegeven voor het verwerken van bijzondere informatie. Onder verwerken wordt verstaan elke handeling of elk geheel van handelingen met betrekking tot informatie, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Mandatering van toestemmingverlening is mogelijk en kan voor verschillende rubriceringsniveaus verschillend worden ingevuld.

Voor bijzondere informatie en informatiesystemen wordt, onder andere ten behoeve van die centrale afweging, in het ministeriële integrale beveiligingsbeleid beschreven op welke wijze bepaald wordt met welke dreigingen (onderkend of voorspelbaar) en welke risico's (voorstelbaar) rekening gehouden moet worden. Alsmede hoe dit overzicht van dreigingen en risico's actueel gehouden wordt.

Voor internationale bijzondere informatie geldt een andere procedure. Voordat dergelijke informatie mag worden verwerkt is in lijn met artikel 6 lid 3 van dit voorschrift, tevens toestemming nodig van de NSA.

Onder c:

Behalve de initiële toestemming voor de verwerking van bijzondere informatie stelt het VIRBI 2013 in de bijlage ook eisen aan het toezicht tijdens de verwerking. Hierbij wordt een minimale frequentie van toezicht gegeven die hoger is naarmate het rubriceringsniveau ook hoger ligt. Ook worden voor Stg. Confidentieel en hoger gerubriceerde informatie eisen gesteld aan de administratie met betrekking tot kennisname.

Zoals in het BVR 2013, artikel 5, lid 1, is vastgelegd is het lijnmanagement verantwoordelijk voor de integrale beveiliging van hun dienstonderdeel. De BVA heeft namens de secretaris-generaal de centrale toezichthoudende rol (BVR 2013, artikel 4, lid 3). De voor het toezicht noodzakelijke onafhankelijke toetsing kan door derden (bijvoorbeeld de auditfunctie van de Rijksdienst) worden ingevuld.

Nadere invulling van de toewijzing van verantwoordelijkheden voor ketens van informatiesystemen

Het VIR bepaalt dat de verantwoordelijkheid voor ketens van informatiesystemen aan lijnmanagers wordt toegewezen. Het VIRBI 2013 stelt eisen aan de beveiliging van bijzondere informatie, ook die in ketens wordt verwerkt.

De functionaris onder wiens verantwoordelijkheid de bijzondere informatie wordt verwerkt zorgt er voor en ziet erop toe dat de beveiliging van de bijzondere informatie in overeenstemming met de eisen wordt ingericht, ook door de lijnmanagers die verantwoordelijk zijn voor de ketens van informatiesystemen voordat de bijzondere informatie daarin wordt opgenomen. Ook waar delen van ketens zich buiten de rijksdienst bevinden dient zekerheid te bestaan dat aan de beveiligingseisen is voldaan.

Artikel 4 Rubriceringen

In de Wet bescherming staatsgeheimen is in de titel aangegeven dat Staatsgeheimen gegevens betreffen waarvan de geheimhouding door het belang van de Staat wordt geboden. In artikel IIA van de Wet bescherming staatsgeheimen is opgenomen dat onder de veiligheid van de Staat ook wordt verstaan de veiligheid van diens bondgenoten. Informatie waarvan de geheimhouding is geboden door het belang van één of meerdere ministeries en niet als Staatsgeheim is gerubriceerd, wordt als Departementaal Vertrouwelijk gerubriceerd.

De inschaling van de rubricering wordt op basis van twee criteria bepaald: schade en belang.

Schade

De mate van schade aan een belang is mede bepalend voor de hoogte van de rubricering. Uitgegaan is van de volgende criteria in oplopende volgorde:

- a. Schade: beperkte nadelige invloed;
- b. Ernstige schade: nadelige invloed, korte termijn geen alternatieven;
- c. Zeer ernstige schade: onmisbaar, geen alternatieven mogelijk.

Belang

De mate van vitaliteit van de belangen voor de Staat of haar bondgenoten of een belang van een of meerdere ministeries is mede bepalend voor de hoogte van de rubricering. Voor de bepaling van de (vitale) belangen van de Staat en/of haar bondgenoten is aangesloten op de vijf onderscheiden vitale belangen in de Strategie Nationale Veiligheid (Tweede Kamer, vergaderjaar 2006–2007, 30 821, nr. 3), die de basis is voor de Rijksbrede aanpak van de nationale veiligheid. Deze vitale belangen zijn als volgt gedefinieerd:

- a. territoriale veiligheid: het ongestoord functioneren van Nederland als onafhankelijke staat, en in het bijzonder de territoriale integriteit van het grondgebied en de internationale positie;
- b. fysieke veiligheid: het ongestoord functioneren van de mens in Nederland en zijn omgeving;
- c. economische veiligheid: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie;
- d. ecologische veiligheid: het beschikken over voldoende zelfherstellend vermogen van de leefomgeving bij aantasting;
- e. sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden.

Belang van een of meerdere ministeries betreffen het ongestoord functioneren van het ministerie in de uitvoering van haar taken of ter realisatie van haar doelen.

Conform de transitietabel in de toelichting bij artikel 2, wordt bijzondere informatie gerubriceerd door NAVO en EU beveiligd volgens het overeenkomstige nationale beveiligingsniveau.

Een rubricering kan aangevuld worden door een of meerdere merkingen. Hiermee kan een specifieke beperking van de kring van gerechtigden worden aangegeven. Merkingen staan echter los van de rubricering van de informatie en dit onderwerp is daarom niet opgenomen in deze regeling.

Lid 2, onder a, b en c:

Benadrukt wordt de aansluiting met artikel 98 en verder van het Wetboek van Strafrecht, dat de strafbaarheid regelt van misdrijven met betrekking tot staatsgeheimen, zoals het ongeautoriseerd toegang proberen te verkrijgen tot of het onzorgvuldig behandelen van staatsgeheimen. Artikel 98 en verder van het Wetboek van Strafrecht hanteert de term 'een inlichting'; de in het VIRBI 2013 gebruikte term 'informatie' sluit de term 'een inlichting' in.

Lid 2, onder d:

Departementaal Vertrouwelijk gerubriceerde informatie betreft primair het belang van één of meerdere ministeries. De maatschappelijke consequenties als gevolg van ongeautoriseerde kennisname blijven voor dit rubriceringsniveau beperkt in tijd en omvang.

Lid 3:

Het vaststellen van rubricering gebeurt expliciet met het vaststellen van de inhoud of de informatie. En eveneens (mondeling) bij vergaderingen of andere gesprekken. Daarnaast kunnen databases en informatiesystemen door de (proces)eigenaar in zijn geheel gerubriceerd worden, waarmee dit ook geldt voor de opgenomen/ingevoerde informatie.

In de conceptfase wordt de informatie behandeld conform het niveau van beveiliging gekoppeld aan het voorstel tot rubricering van de steller, totdat het definitieve niveau van rubricering is bepaald door degene die de inhoud vaststelt, waarna de beveiliging conform het vastgestelde rubriceringsniveau wordt behandeld.

Artikel 5 Herzien en beëindigen van de rubricering

De geheimhouding van bijzondere informatie is noodzakelijk voor een specifieke periode of verbonden aan een bepaalde gebeurtenis, maar zal niet automatisch vervallen. De rubricering wordt daarom altijd aangevuld met een maximum tijdsverloop of bepaalde gebeurtenis, na dit tijdsverloop of de bepaalde gebeurtenis dient de noodzaak tot en de hoogte van de rubricering opnieuw te worden

vastgesteld. Hiermee wordt enerzijds voorkomen dat informatie onnodig lang beveiligd wordt en anderzijds wordt de geheimhouding van informatie geborgd zolang dit noodzakelijk is. Er kan eventueel een verzoek worden ingediend, door personen die geautoriseerd zijn om kennis te nemen van die informatie, bij de vaststeller van de rubricering van de informatie, om te voorkomen dat informatie onnodig gerubriceerd blijft.

Bij een verzoek in het kader van de Wet Openbaarheid Bestuur (WOB) wordt op grond van artikel 5 de rubricering opnieuw beoordeeld. De rubricering van de informatie of delen daarvan moet (en) worden beëindigd als de belangen niet onder de uitzonderingsgronden van de WOB vallen. Informatie die wordt vrijgegeven op basis van een dergelijk verzoek kan immers niet langer gerubriceerd zijn. Indien delen niet worden gederubriceerd, moeten deze onleesbaar worden gemaakt in, dan wel verwijderd uit het vrij te geven document.

Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen en Staatsgeheimen die door de wet als zodanig zijn aangewezen, vallen buiten dit regime. Bijzondere informatie die krachtens een internationaal verdrag is verkregen, heeft per definitie een niet Nederlandse rubricering. De informatie dient overeenkomstig de in het verdrag overeengekomen beveiligingsregime te worden beveiligd. Indien de informatie niet meer nodig is, kan deze worden teruggestuurd of worden vernietigd. Informatie die door de wet als zodanig is aangewezen, valt eveneens buiten het gestelde in het eerste lid van dit artikel. De Kernenergiewet en het Geheimhoudingsbesluit Kernenergiewet, KB 17 juni 1971 zijn hiervan voorbeelden.

Uitsluitend de vaststeller van de rubricering is bevoegd de rubricering te herzien of te beëindigen. De vaststelling is functie- en niet persoonsgebonden. De vaststeller van de informatie blijft ook na reorganisaties (onderbrengen bij een ander deel van of buiten de Rijksdienst) of overdracht van functies naar een ander deel van of buiten de Rijksdienst, de zorgplicht houden voor de bijzondere informatie, tenzij expliciet vóór een dergelijke reorganisatie of functieoverdracht is bepaald dat de zorgplicht ook over gaat. Indien de zorgplicht niet over gaat, zal de zorgdrager bij een voornemen of plicht tot herziening of beëindiging van de rubricering overleg voeren met de nieuwe procesverantwoordelijke waar de organisatie of functie is ondergebracht.

Omdat uitsluitend de oorspronkelijke rubriceerder mag herrubriceren, behoudt afgeleid werk de oorspronkelijke rubricering van het gebruikte bronmateriaal, tenzij in overeenstemming met de oorspronkelijke rubriceerder een andere rubricering kan worden vastgesteld. Het is dus niet zonder meer toegestaan om uittreksels of overzichten lager te rubriceren dan het bronmateriaal dat hiervoor gebruikt is. Uitsluitend de SG van het ministerie dat de oorspronkelijke rubricering heeft vastgesteld kan functionarissen mandateren om de rubricering te herzien.

Lid 4 is vooral bedoeld als herinnering. In de Archiefwet 1995 (artikel 14) is bepaald dat archiefbescheiden die in een archiefbewaarplaats berusten, behoudens het bepaalde in de artikelen 15, 16 en 17, openbaar zijn. De rubricering vervalt dus bij overbrenging naar een rijksarchiefbewaarplaats, tenzij de zorgdrager besluit dat de rubricering ook in de archiefbewaarplaats geldt, gelet op de belangen die in artikel 15, eerste lid van de Archiefwet 1995 staan opgesomd. Bij overbrenging is het op grond van de Archiefwet 1995 de zorgdrager, i.c. de minister, die de beperkingen aan de openbaarheid vaststelt, na advies van de algemene rijksarchivaris. Relevant is in dergelijke gevallen de eisen aan de beveiliging die de zorgdrager (eigenaar van de informatie) stelt ook expliciet kenbaar te maken. De beheerder van de archiefbewaarplaats is eveneens gehouden aan het VIR 2007 en, voor zover het bijzonder informatie betreft, het VIRBI 2013.

Artikel 6 Eisen aan de beveiliging

Lid 2:

Bij gebruik van de afwijkingsruimte gegeven in het tweede lid dienen in de verantwoording van de afwijking de beveiligingsdoelstellingen te worden meegewogen, conform het principe 'pas toe of leg uit'.

Onder risicomanagement wordt verstaan het in een inzichtelijk afwegingsproces bepalen van de beveiligingsmaatregelen, waarbij de maatregelen proportioneel, efficiënt en effectief zijn in relatie tot de belangen, de reële dreigingen en onderkende risico's. Hierbij wordt ook inzichtelijk gemaakt welke restrisico's worden geaccepteerd. Met betrekking tot de dreiging van specifieke tegenstanders, hun capaciteiten en modus operandi kan de BVA informatie aanreiken. Een deel van de informatie betreft de BVA van de AIVD, de MIVD, de NCTV en andere niet voor een ieder toegankelijke bronnen die op dit terrein een taak hebben. Het geheel wordt zo opgezet dat verantwoording afgelegd kan worden over de gemaakte keuzes en het bereikte beveiligingsniveau. In de bijlage worden de eisen die aan de



vertrouwelijkheid worden gesteld nader benoemd. Specifiek voor de beveiliging van bijzondere informatie geldt dat voor de toepassing en naleving van de eis van vertrouwelijkheid (exclusiviteit) een dusdanige set van maatregelen zijn toegepast dat de risico's die de verwerking en de aard van de te beschermen bijzondere informatie met zich meebrengen, adequaat zijn afgedekt. Dit wordt aangeduid als een positief beveiligingsrendement.

Lid 3 geeft aan dat er op basis van internationale verdragen of internationale overeenkomsten beperkingen bestaan waardoor voor de beveiliging van betreffende bijzondere informatie verantwoording aan een andere autoriteit verschuldigd is. Het betreft hier de NSA.

Artikel 7 Buiten de rijksdienst brengen van bijzondere informatie

Het kan noodzakelijk zijn om bijzondere informatie buiten de rijksdienst te brengen. Hiervan is sprake zodra de informatie ter beschikking wordt gesteld aan mensen of instanties waarop het VIRBI 2013 niet van toepassing is, dus zodra zij buiten de reikwijdte gesteld in artikel 2 lid 1 van dit voorschrift vallen. De lijnmanager die verantwoordelijk is voor de informatie dient zorg te dragen voor een toereikende beveiliging en te voorzien in de mogelijkheid en bevoegdheid om toezicht en controle hierop uit te oefenen, alvorens de betreffende bijzondere informatie buiten de rijksdienst wordt gebracht. Bijzondere informatie wordt uitsluitend buiten de rijksdienst gebracht indien de secretaris-generaal, of de door hem aangewezen ambtenaar, vooraf toestemming heeft verleend. Bij structurele informatieoverdracht naar externe partijen kan door het ministerie een generieke regeling worden getroffen, waarmee de voorwaarden centraal worden vastgelegd. Daar waar noodzakelijkerwijs informatie door omstandigheden direct buiten de Rijksdienst moet worden gebracht, wordt achteraf verantwoording afgelegd over de noodzaak en de getroffen maatregelen.

Artikel 8 Compromittering van bijzondere informatie

De BVA of de aangewezen beveiligingscoördinatoren (BVR 2013), zijn het eerste en centrale aanspreekpunt bij mogelijke incidenten met bijzondere informatie. De BVA kan verschillende meldingen aan elkaar relateren, heeft de mogelijkheden om een goede eerste inschatting te maken van de aard en omvang van een eventueel incident, heeft op grond van het BVR 2013 directe toegang tot de secretaris-generaal en de bevoegdheid om aanwijzingen te geven voor de eerste schadebeperkende en beveiligingsherstellende maatregelen.

Waar het staatsgeheimen betreft, informeert de BVA, indien bij eerste beschouwing daadwerkelijk sprake lijkt te zijn van een ongeautoriseerde kennisname, direct de secretaris-generaal. Deze bepaalt aan de hand van de situatie en op advies van de BVA de wijze waarop het verdere onderzoek naar het incident dient te worden ingevuld.

Waar de BVA het eerste en centrale aanspreekpunt binnen het ministerie vormt, heeft de AIVD deze rol voor de gehele rijksdienst met uitzondering van het ministerie van Defensie. Centrale melding van vermoedelijke en feitelijke ongeautoriseerde kennisname maakt het mogelijk om trends en verbanden te ontdekken binnen deze meldingen.

Waar andere partijen schade kunnen krijgen als gevolg van de (vermoedelijke) ongeautoriseerde kennisname van bijzondere informatie worden deze partijen geïnformeerd en betrokken bij het onderzoek. Voor internationale informatie geldt dat de NSA medezeggenschap heeft over het onderzoek.

Artikel 9 Commissie van onderzoek

Deze commissie bestaat uit één of meer ambtenaren die met het uitvoeren van onderzoeken ervaring hebben, die niet betrokken zijn bij de compromittering en die niet onmiddellijk ondergeschikt zijn aan bij de compromittering betrokken ambtenaren. De commissie is gerechtigd kennis te nemen van de informatie die op de compromittering betrekking heeft en de bij de compromittering betrokken ambtenaren, alsmede de ambtenaar die de rubricering heeft vastgesteld, te horen. Het rapport van bevindingen dient te worden beoordeeld op de noodzaak tot rubricering.

Voordat een interne commissie van onderzoek van start gaat wordt expliciet de afweging gemaakt of sprake is van een strafbaar feit in welk kader aangifte vereist is. Er wordt dan geen zelfstandig intern onderzoek opgestart, wel wordt direct bepaald in overleg met de opsporingsinstantie of en zo ja, welke gegevens veilig gesteld moeten worden en op welke wijze dit gebeurt.

Het is van belang om ten behoeve van het uitvoeren van dergelijke onderzoeken gebruik te kunnen maken van expertise op Rijksniveau. De BVA's kunnen dan een beroep doen op hun collega's om hen



bij te staan en te ondersteunen in een dergelijk onderzoek.
De Algemene Inlichtingen- en Veiligheidsdienst of de Militaire Inlichtingen- en Veiligheidsdienst kunnen de commissie bij haar onderzoek terzijde staan.

Artikel 10 Slotbepaling

Lid 2:

Reeds bestaande gerubriceerde informatie hoeft niet als gevolg van de inwerkingtreding van het VIRBI 2013 opnieuw te worden beoordeeld en gerubriceerd. Dit wordt uiterlijk 10 jaar na vaststelling door de vaststeller of diens rechtsopvolger onderzocht.

*De Minister-President, Minister van Algemene Zaken,
M. Rutte.*



Bijlage 8

Uitspraak Raad van State

201708297/1/A3 ECLI:NL:RVS::2019:100

Uitspraak 201708297/1/A3

Datum van uitspraak: woensdag 16 januari 2019
Tegen: de minister van Algemene Zaken
Proceduresoort: Hoger beroep
Rechtsgebied: Openbaarheid
ECLI: **ECLI:NL:RVS:2019:100**

201708297/1/A3.

Datum uitspraak: 16 januari 2019

AFDELING
BESTUURSRECHTSPRAAK

Uitspraak op de hoger beroepen van:

1. de minister van Algemene Zaken,
2. RTL Nieuws, onderdeel van RTL Nederland B.V., gevestigd te Hilversum, appellanten,

tegen de uitspraak van de rechtbank Midden-Nederland van 7 september 2017 in zaak nr. 16/5602 in het geding tussen:

RTL Nieuws

en

de minister.

Procesverloop

Bij besluit van 22 juni 2016 heeft de minister beslist op een verzoek van RTL Nieuws om openbaarmaking van informatie over de ramp met vlucht MH17 op grond van de Wet openbaarheid van bestuur (hierna: Wob).

Bij besluit van 28 oktober 2016 heeft de minister het door RTL Nieuws daartegen gemaakte bezwaar ongegrond verklaard.

Bij tussenuitspraak van 3 april 2017 heeft de rechtbank de minister opgedragen binnen twee weken aan de rechtbank mee te delen of hij gebruik maakt van de gelegenheid de geconstateerde gebreken in het besluit van 28 oktober 2016 te herstellen, de minister in de gelegenheid gesteld om binnen vier weken na verzending van de tussenuitspraak de geconstateerde gebreken te herstellen met inachtneming van de overwegingen en aanwijzingen in de tussenuitspraak en iedere verdere beslissing aangehouden. Deze uitspraak is aangehecht.

Bij uitspraak van 7 september 2017 heeft de rechtbank het door RTL Nieuws tegen het besluit van 28 oktober 2016 ingestelde beroep gegrond verklaard, dat besluit vernietigd en de minister opgedragen binnen zes weken na de dag van verzending van haar uitspraak een nieuw besluit te nemen op het bezwaar van RTL Nieuws met inachtneming van haar einduitspraak en tussenuitspraak. Deze uitspraak is aangehecht.

Tegen de tussenuitspraak van 3 april 2017 en de einduitspraak van 7 september 2017 hebben de minister en RTL Nieuws hoger beroep ingesteld.

De minister heeft een schriftelijke uiteenzetting gegeven.

RTL Nieuws heeft de toestemming als bedoeld in artikel 8:29, vijfde lid, van de Algemene wet bestuursrecht (hierna: de Awb), verleend.

De minister heeft bij besluit van 4 december 2017 opnieuw op het bezwaar tegen het besluit van 22 juni 2016 beslist.

De Afdeling heeft de zaak ter zitting behandeld op 3 december 2018, waar de minister, vertegenwoordigd door mr. K.J. Bregman, bijgestaan door mr. E.C. Pietermaat, advocaat te Den Haag, en RTL Nieuws, vertegenwoordigd door [gemachtigden], zijn verschenen.

Overwegingen

Wettelijk kader

1. De relevante wet- en regelgeving is vervat in een bijlage bij deze uitspraak. Deze bijlage maakt deel uit van de uitspraak.

Het Wob-verzoek

2. RTL Nieuws heeft de minister bij brief van 15 februari 2016 op grond van de Wob verzocht om openbaarmaking van de "geobjectiveerde verslagen van de bijeenkomsten van de ministerraad op 23 juli 2014, 27 juli 2014 en 15 augustus 2014" zoals genoemd op bladzijde 58 van het rapport van de Universiteit Twente van 9 december 2015 over de evaluatie van de nationale crisisbeheersingsorganisatie naar aanleiding van de ramp met vlucht MH17. Voorts heeft RTL Nieuws verzocht om openbaarmaking van het geaccordeerde verslag van het gesprek dat de minister met de onderzoekers van de Universiteit Twente in het kader van voornoemd onderzoek heeft gevoerd.

Besluitvorming minister

3. De minister heeft naar aanleiding van het verzoek RTL Nieuws bericht dat hij twee documenten heeft aangetroffen. Dit zijn een notitie met daarin de geobjectiveerde verslagen van de bijeenkomsten van de ministerraad van 23 juli, 27 juli en 15 augustus 2014 en een verslag van het gesprek dat de minister-president op 8 september 2015 met de onderzoekers van de Universiteit Twente heeft gevoerd.

De minister heeft openbaarmaking van deze documenten integraal geweigerd. Hij heeft daaraan ten grondslag gelegd dat het belang van openbaarmaking van de verzochte documenten niet opweegt tegen onder meer het belang van de betrekkingen van Nederland met andere staten als bedoeld in artikel 10, tweede lid, aanhef en onder a, van de Wob.

Voorts heeft de minister aan de weigering ten grondslag gelegd dat het belang van openbaarmaking van de documenten niet opweegt tegen het belang van het voorkomen van onevenredige benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden als bedoeld in artikel 10, tweede lid, aanhef en onder g, van de

Wob. In dit verband heeft de minister over de notitie met geobjectieerde verslagen van de ministerraad betoogd dat een vrije en onbelemmerde uitwisseling van argumenten van wezenlijk belang is voor het goed kunnen uitvoeren van de grondwettelijke taak en werkzaamheden van de ministerraad. Openbaarmaking van deze informatie leidt volgens de minister tot een onevenredige benadeling, omdat dit de open en ongedwongen beraadslaging tussen de leden van de ministerraad en daarmee de besluitvorming over het algemeen regeringsbeleid en de bevordering van de eenheid daarvan, belemmert en schade toebrengt. Het feit dat de verslagen geobjectieerd zijn, vormt volgens de minister geen aanleiding om tot een ander oordeel te komen dan wanneer dit niet het geval was geweest.

Over het gespreksverslag van 8 september 2015 heeft de minister erop gewezen dat in het gespreksprotocol tussen hem en de Universiteit Twente is opgenomen dat dit verslag niet door derden opvraagbaar is, ook niet nadat het onderzoek is afgerond. De geïnterviewden mochten er daarom van uitgaan dat de gesprekken met de onderzoekers in alle vertrouwelijkheid zouden plaatsvinden. Indien de verslagen achteraf alsnog openbaar zouden worden gemaakt, zou deze vertrouwelijkheid feitelijk komen te vervallen. Voorts kan openbaarmaking de onderzoekers van de Universiteit Twente onevenredig benadelen. Deze benadeling is gelegen in de omstandigheid dat de onderzoekers het verwijt kan worden gemaakt dat de gedane toezegging van absolute vertrouwelijkheid niet is nageleefd en, daarmee samenhangend, dat toekomstig onderzoek hierdoor ernstig kan worden bemoeilijkt. Als de vertrouwelijkheid die de onderzoekers aan de gesprekspartners hebben toegezegd in de praktijk zinledig blijkt te zijn, dan zal dat immers leiden tot een afname van de bereidheid om in toekomstige situaties informatie met een onderzoekscommissie te delen. De afname van de bereidheid om mee te werken aan onafhankelijk onderzoek is volgens de minister temeer aannemelijk indien, zoals in dit geval, het onderzoek betrekking heeft op een gevoelig onderwerp dat kan rekenen op grote belangstelling van zowel de politiek als de journalistiek. Ten slotte heeft de minister aan de weigering om het gespreksverslag openbaar te maken ten grondslag gelegd dat dit persoonlijke beleidsopvattingen voor intern beraad bevat als bedoeld in artikel 11, eerste lid, van de Wob. Het is niet in het belang van een goede en democratische bestuursvoering indien de in het gespreksverslag opgenomen standpunten zelfstandig zouden worden betrokken in de publieke discussie, aldus de minister.

Tussenuitspraak rechtbank 3 april 2017

4. In haar tussenuitspraak heeft de rechtbank over de geobjectieerde verslagen van de ministerraad overwogen dat zij grotendeels de minister volgt in zijn standpunt dat artikel 10, tweede lid, aanhef en onder g, van de Wob zich tegen openbaarmaking verzet. Openbaarmaking van de verslagen geeft teveel inzicht in wat in de ministerraad vertrouwelijk is besproken en zou volgens de rechtbank leiden tot onevenredige benadeling van de ministerraad. Dit geldt evenwel niet voor de laatste zin van het geobjectieerde verslag van de bijeenkomst van de ministerraad op 15 augustus 2014. Het belang dat de minister heeft bij vertrouwelijk overleg over de nasleep van de MH17-ramp lijkt hier volgens de rechtbank toepassing te missen. De gegeven motivering dat artikel 10, tweede lid, aanhef en onder g, van de Wob aan openbaarmaking van deze laatste zin in de weg zou staan, volgt de rechtbank zonder nadere motivering niet. De minister moet daarom beter toelichten waaruit volgens hem de onevenredige benadeling zou bestaan.

De rechtbank heeft voorts overwogen dat de minister de integrale weigering om het gespreksverslag van de onderzoekers van de Universiteit Twente openbaar te maken evenmin voldoende heeft gemotiveerd. De minister heeft niet kunnen volstaan met een algemene verwijzing naar het gespreksprotocol van de Universiteit Twente, het persoonlijk belang van de geïnterviewde en het belang van het onderzoek en de onderzoekers. Geen van de door de minister ingeroepen weigeringsgronden, te weten de weigeringsgronden van artikel 10, tweede lid, aanhef en onder a en g en artikel 11, eerste lid, van de Wob, kan het gehele document beslaan en de minister zal daarom nader moeten toelichten welke weigeringsgronden hij van toepassing acht op de verschillende tekstgedeeltes van het gespreksverslag, waarbij hij per tekstgedeelte een belangafweging moet maken, aldus de rechtbank.

De rechtbank heeft aanleiding gezien om de minister de gelegenheid te geven de hiervoor genoemde gebreken te herstellen.

Einduitspraak rechtbank 7 september 2017

5. De rechtbank heeft in de einduitspraak vastgesteld dat de minister geen gebruik heeft gemaakt van de mogelijkheid de door rechtbank geconstateerde gebreken te herstellen. Gelet op hetgeen de rechtbank in de tussenuitspraak heeft overwogen, heeft de rechtbank het beroep gegrond verklaard, het besluit van 28 oktober 2016 wegens strijd met artikel 7:12, eerste lid, van de Awb vernietigd en de minister opgedragen een nieuw besluit op bezwaar te nemen.

6. Tegen de tussenuitspraak en de einduitspraak hebben zowel de minister als RTL Nieuws hoger beroep ingesteld.

Hoger beroep minister

7. De minister betoogt dat de rechtbank ten onrechte heeft geoordeeld dat hij onvoldoende heeft gemotiveerd waarom de laatste zin van het geobjectiveerde verslag van de ministerraad van 15 augustus 2014 en het volledige gespreksverslag niet openbaar kunnen worden gemaakt.

Over het geobjectiveerde verslag van de ministerraad van 15 augustus 2014 voert de minister aan dat de rechtbank ten onrechte een onderscheid heeft aangebracht tussen de laatste zin en de rest van het verslag. Volgens de minister leidt openbaarmaking van de laatste zin van het verslag ertoe dat inzicht zou worden verschaft in wat in de ministerraad vertrouwelijk is besproken, hetgeen tot onevenredige benadeling van de ministerraad leidt. In dit verband benadrukt de minister dat hij in zijn besluitvorming heeft gewezen op het bepaalde in artikel 45 van de Grondwet en artikel 26, eerste lid, van het reglement van orde voor de ministerraad, waaruit de grondwettelijke taak voor de ministerraad volgt om de eenheid van het regeringsbeleid te bevorderen en de noodzaak dat het beraad binnen de ministerraad vertrouwelijk blijft. De minister verwijst naar de uitspraak van de Afdeling van 25 oktober 2017, [ECLI:NL:RVS:2017:2883](#).

Over het gespreksverslag voert de minister onder verwijzing naar jurisprudentie van de Afdeling aan dat de rechtbank ten onrechte niet heeft onderkend dat vanwege het belang dat is gemoeid met toekomstig onderzoek, het noodzakelijk is dat de toegezegde vertrouwelijkheid wordt gerespecteerd en daarom het gespreksverslag in zijn geheel niet openbaar kan worden gemaakt. Aannemelijk is dat als gevolg van openbaarmaking anderen in de toekomst minder bereidwillig zullen zijn om aan dezelfde type onderzoeken mee te werken, dan wel terughoudender zullen worden in hun verklaringen, aldus de minister. Door de onderzoekers van de Universiteit Twente is aan de gesprekspartners absolute vertrouwelijkheid toegezegd. In de wetenschap dat wat zij aan de onderzoekers zouden toevertrouwen niet openbaar zou worden gemaakt, hebben de geïnterviewden met grote openheid over de gebeurtenissen na de ramp met MH17 verteld en de vragen van de onderzoekers beantwoord. Mede daardoor kon een goede evaluatie van het functioneren van de nationale crisisbeheersingsorganisatie plaatsvinden. Het is zeer aannemelijk dat als, naar achteraf blijkt, de toegezegde vertrouwelijkheid niet kan worden gegarandeerd, men in de toekomst terughoudender zal worden ten aanzien van hetgeen aan onderzoekers kan worden toevertrouwd, hetgeen tot onevenredige benadeling van de Staat leidt. Vanwege het belang dat ermee is gemoeid dat te voorkomen, mocht de minister op grond van artikel 10, tweede lid, aanhef en onder g, en artikel 11 van de Wob de openbaarmaking van het gespreksverslag weigeren, aldus de minister.

Hoger beroep RTL Nieuws

8. RTL Nieuws betoogt dat de rechtbank bij de beoordeling van de geobjectiveerde verslagen van de ministerraad ten onrechte is uitgegaan van de aanname dat deze verslagen te vergelijken zijn met normale verslagen van de ministerraad. Omdat de verslagen geobjectiveerd zijn, is er voor de toepassing van de weigeringsgronden van de Wob geen ruimte, aldus

9. RTL Nieuws betoogt voorts dat zij als persorgaan op grond van artikel 10 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) een grotere aanspraak heeft op openbaarmaking van de verzochte documenten. In dit verband wijst zij op het arrest van het Europees Hof voor de Rechten van de Mens van 8 november 2016, [ECLI:CE:ECHR:2016:1108JUD001803011](#), Magyar Helsinki Bizottság tegen Hongarije (hierna: het MHB-arrest) en voornoemde uitspraak van de Afdeling van 25 oktober 2017, waaruit volgt dat aan artikel 10 van het EVRM een zelfstandige betekenis toekomt. Zij wijst er voorts op dat gelet op de impact van de ramp met de MH17 het maatschappelijk belang bij openbaarmaking groot is.

Beoordeling Afdeling

10. De Afdeling heeft met toepassing van artikel 8:29 van de Awb kennis genomen van de stukken.

- Geobjectiveerde verslagen ministerraad -

11. Ingevolge artikel 10, tweede lid, aanhef en onder g, van de Wob blijft het verstrekken van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden. Dit artikel beschermt tevens het belang bij het voorkomen van onevenredige benadeling van de overheid.

De Afdeling overweegt dat in het reglement van orde voor de ministerraad de werkwijze van de ministerraad is vastgelegd. Ingevolge artikel 26, eerste lid, van dat reglement bestaat ten aanzien van hetgeen ter vergadering van de ministerraad wordt besproken of geschiedt een geheimhoudingsplicht. In de nota van toelichting (Stb. 1994, 203, blz. 23) is vermeld dat de grote zorg voor geheimhouding van hetgeen in de raad aan de orde komt vooral zijn oorzaak vindt in de opdracht aan de raad de eenheid van het regeringsbeleid te bevorderen. Het bekend worden van individuele standpunten van bewindspersonen in die raad zou aan die eenheid afbreuk kunnen doen, aldus de toelichting.

De minister heeft terecht gewezen op het belang dat toekomt aan artikel 26 van het reglement van orde voor de ministerraad en de toelichting op deze bepaling, mede in het licht van de eenheid van het algemeen regeringsbeleid als bedoeld in artikel 45, derde lid, van de Grondwet. Hierbij is van betekenis dat de overheid er groot belang bij heeft dat deelnemers aan de ministerraad onbelemmerd met elkaar kunnen spreken over, in dit geval, de ramp met vlucht MH17. Daarvoor is noodzakelijk dat hetgeen in de vergaderingen is besproken vertrouwelijk blijft, zoals de Afdeling heeft overwogen in de uitspraak van 25 oktober 2017, [ECLI:NL:RVS:2017:2883](#).

De Afdeling volgt de minister dan ook in zijn standpunt dat openbaarmaking van de geobjectiveerde verslagen van de ministerraad er toe leidt dat het goed functioneren van de ministerraad in het gedrang komt. Het is aannemelijk dat openbaarmaking ertoe leidt dat deelnemers aan de ministerraad in de toekomst terughoudender zullen zijn met hetgeen zij in die vergaderingen bespreken. De overheid heeft er belang bij dat de deelnemers aan de ministerraad vrijelijk en in vertrouwen kunnen spreken en vrijelijk kunnen bepalen wat zij aan de orde stellen. Dit belang zou door openbaarmaking onevenredig worden benadeeld. Dat het in dit geval gaat om verslagen die worden aangeduid als "geobjectiveerde verslagen" maakt het voorgaande niet anders, omdat ook deze verslagen gedetailleerd inzicht verschaffen in hetgeen in de ministerraad is besproken. Er bestaat geen aanleiding ten aanzien van de laatste zin van het verslag een andere benadering te volgen.

Gegeven het geldende geheimhoudingsregime, de opdracht om de eenheid van het regeringsbeleid te bevorderen en de gevoelige aard van de onderwerpen die binnen de ministerraad worden besproken, heeft de minister ten aanzien van de volledige verslagen het belang om onevenredige benadeling te voorkomen dan ook zwaarder mogen laten wegen dan het belang dat is gemoeid met openbaarmaking.

Gelet op het vorenstaande heeft de rechtbank ten onrechte geoordeeld dat de minister onvoldoende heeft gemotiveerd waarom de laatste zin van het geobjectiveerde verslag van de ministerraad van 15 augustus 2014 niet openbaar kan worden gemaakt.

Het betoog van de minister slaagt.

11.1. Gelet op hetgeen de Afdeling hiervoor in overweging 11 heeft overwogen, faalt het betoog van RTL Nieuws.

- Het gespreksverslag van de Universiteit Twente -

12. Na het neerstorten van het vliegtuig van vlucht MH17 van Malaysia Airlines in Oekraïne op 17 juli 2014 trad de Nederlandse crisisbeheersingsorganisatie in werking, zoals die is vastgelegd in het op 12 april 2013 vastgestelde Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbesluitvorming. In het Nationaal Handboek Crisisbesluitvorming is opgenomen dat ieder optreden van de crisisbeheersingsorganisatie wordt geëvalueerd. De minister van Veiligheid en Justitie (thans: de minister van Justitie en Veiligheid) heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum verzocht om een onafhankelijk evaluatieonderzoek te laten uitvoeren naar de crisisbeheersing rond de ramp met vlucht MH17. Dit onafhankelijke onderzoek is uitgevoerd door onderzoekers van de Universiteit Twente. De onderzoekers hebben, om toegang tot vertrouwelijke informatie te krijgen en om te kunnen spreken met zogeheten sleutelinformanten, een geheimhoudingsverklaring getekend. Daarmee is mede beoogd te bevorderen dat de gesprekken in vertrouwelijkheid konden plaatsvinden. Deze vertrouwelijkheid is vervolgens voorafgaand aan de interviews door de onderzoekers aan de geïnterviewden toegezegd. Het gespreksverslag betreft een interview dat de minister heeft gegeven aan onderzoekers van de Universiteit Twente in het kader van deze evaluatie. De onderzoekers hebben in het openbaar gemaakte rapport "Evaluatie nationale crisisbeheersingsorganisatie vlucht MH17" van 9 december 2015 gedeeltelijk de interviews met verschillende informanten, waaronder die met de minister, op niet naar personen herleidbare wijze opgenomen.

De overheid heeft er baat bij dat bij een evaluatie zo veel mogelijk informatie wordt verkregen om daaruit lering te trekken voor een volgende crisis. Dit geldt temeer in een situatie als deze waarbij het gaat om de evaluatie van de crisisbeheersingsorganisatie rondom een nationale ramp die een grote impact op de samenleving heeft. Het is in het belang van de evaluatie dat informanten zo vrijelijk mogelijk verklaren en niet uit vrees voor openbaarmaking volstaan met het verklaren van het hoogst noodzakelijke. Openbaarmaking van het gespreksverslag zou er toe kunnen leiden dat de bereidheid van informanten om in toekomstige gevallen informatie te delen met onafhankelijke onderzoekers zal afnemen en dat, uit vrees dat ook dan niet zal worden vastgehouden aan de toegezegde vertrouwelijkheid, informanten voor het onderzoek relevante informatie voor zich zullen houden. De minister heeft gelet op de toegezegde vertrouwelijkheid dan ook van belang mogen achten dat de informanten er niet op bedacht behoeften te zijn dat hun verklaringen als zodanig openbaar zouden worden gemaakt. De Afdeling is daarom van oordeel dat de minister zich op het standpunt heeft mogen stellen dat openbaarmaking van het gespreksverslag tot onevenredig nadeel van de Staat leidt. De Afdeling is, anders dan de rechtbank, voorts van oordeel dat de minister, gelet op de door hem gegeven motivering, zich op het standpunt heeft mogen stellen dat het belang van openbaarmaking niet opweegt tegen dat van het voorkomen van onevenredige benadeling. Dat het in dit geval een verslag van een gesprek met de minister-president betreft, maakt het voorgaande niet anders, omdat ook aan de minister-president vertrouwelijkheid is toegezegd en ook hij ten behoeve van het onafhankelijke evaluatieonderzoek vrij en openhartig en zonder terughoudendheid moet kunnen verklaren en het goed functioneren van het openbaar bestuur wordt geschaad indien hij dat niet meer zou kunnen.

Voorts komt bij de belangenafweging gewicht toe aan het feit dat de minister in eerdere procedures veel documenten over de MH17-ramp heeft verstrekt en dat ook via andere kanalen, waaronder diverse briefings aan de Tweede Kamer, persconferenties en het rapport van de Universiteit Twente,

veel informatie over de MH17-ramp openbaar is gemaakt, zodat ook zonder openbaarmaking van het gespreksverslag het door de Wob vooronderstelde publieke belang van een goede en democratische bestuursvoering wordt gediend.

Het betoog van de minister slaagt.

- Recht op informatie en artikel 10 EVRM -

13. De Afdeling overweegt dat tussen partijen niet in geschil is dat uit het MHB-arrest volgt dat RTL Nieuws als persorgaan aan artikel 10, eerste lid, van het EVRM een recht op inlichtingen van de overheid kan ontleenen, welk recht overigens is onderworpen aan de beperkingen die ingevolge het tweede lid van artikel 10 van het EVRM daaraan gesteld mogen worden.

Zoals de Afdeling in de uitspraak van 25 oktober 2017 heeft overwogen, vereist artikel 10 van het EVRM niet dat alle informatie verstrekt wordt of openbaar wordt gemaakt en biedt het de mogelijkheid bij wet beperkingen te verbinden aan het verstrekken dan wel openbaar maken van gegevens en documenten. Met de bepalingen betreffende de weigeringsgronden in de Wob is inmenging in het in artikel 10, eerste lid, van het EVRM gewaarborgde recht om inlichtingen van de overheid te ontvangen, bij wet voorzien.

In het algemeen mag ervan worden uitgegaan dat de wetgever bij het formuleren van de weigeringsgronden in de artikelen 10 en 11 van de Wob heeft voorzien in beperkingen die noodzakelijk zijn in een democratische samenleving met het oog op de in artikel 10, tweede lid, van het EVRM genoemde belangen. De weigeringsgronden van de Wob strekken ter bescherming van een of meer van deze belangen. Dit uitgangspunt staat er evenwel niet aan in de weg dat een verzoeker aangeeft dat en waarom in zijn concrete situatie aan dit uitgangspunt niet kan worden vastgehouden. Het ligt dan op de weg van de verzoeker om zeer bijzondere omstandigheden te stellen en aannemelijk te maken die zouden meebrengen dat de verzoeker, ondanks toepassing van de Wob, in de uitoefening van het specifieke recht om op grond van artikel 10, eerste lid, van het EVRM inlichtingen te ontvangen, wordt belemmerd zonder dat dit op grond van artikel 10, tweede lid, van het EVRM is gerechtvaardigd.

De Afdeling is van oordeel dat de minister zich, onder verwijzing naar artikel 10, tweede lid, aanhef en onder g, van de Wob, op het standpunt heeft mogen stellen dat het belang bij openbaarheid niet opweegt tegen het met de weigering beschermde belang, te weten het voorkomen van onevenredige benadeling. Zeer bijzondere omstandigheden die zouden meebrengen dat van een ongerechtvaardigde belemmering als hiervoor bedoeld sprake is, zijn door RTL Nieuws niet aannemelijk gemaakt. De enkele stelling van RTL Nieuws dat zij een persorgaan is, is hiertoe onvoldoende. Voorts heeft het feit dat het maatschappelijke belang bij openbaarmaking groot is, reeds voldoende plaats gekregen in artikel 10 van de Wob en de belangenafweging die met toepassing van dit artikel heeft plaatsgevonden. Bij het voorgaande is van betekenis dat de minister in eerdere procedures veel documenten over de MH17-ramp heeft verstrekt en dat ook via andere kanalen, waaronder diverse briefings aan de Tweede Kamer, persconferenties en het rapport van de Universiteit Twente, veel informatie over de MH17-ramp openbaar is gemaakt.

Het voorgaande betekent dat RTL Nieuws in het licht van artikel 10, tweede lid, van het EVRM niet op onrechtmatige wijze is belemmerd in haar aan artikel 10, eerste lid, van het EVRM ontleende recht om inlichtingen van de overheid te ontvangen.

Het betoog van RTL Nieuws faalt.

Conclusie

14. Het hoger beroep van de minister is gegrond. Het hoger beroep van RTL Nieuws is ongegrond. De aangevallen tussenuitspraak en de aangevallen einduitspraak van de rechtbank dienen te worden

vernietigd. Doende hetgeen de rechtbank zou behoren te doen, zal de Afdeling het door RTL Nieuws bij de rechtbank ingestelde beroep tegen het besluit van 28 oktober 2016 ongegrond verklaren. Het voorgaande betekent dat de weigering van de minister om de geobjectiveerde verslagen van de ministerraad en het gespreksverslag van de minister-president van 8 september 2015 openbaar te maken in stand blijft.

15. Bij besluit van 4 december 2017 heeft de minister, gevolg gevend aan de aangevallen einduitspraak, opnieuw beslist op het bezwaar van RTL Nieuws tegen het besluit van 22 juni 2016. Nu dit besluit is genomen ter uitvoering van de aangevallen einduitspraak, komt door de vernietiging van die uitspraak de grondslag aan dit besluit te ontvallen, zodat het reeds daarom dient te worden vernietigd.

16. Voor een proceskostenveroordeling bestaat geen aanleiding.

Beslissing

De Afdeling bestuursrechtspraak van de Raad van State:

- I. verklaart het hoger beroep van de minister van Algemene Zaken gegrond;
- II. verklaart het hoger beroep van RTL Nieuws ongegrond;
- III. vernietigt de tussenuitspraak van de rechtbank Midden-Nederland van 3 april 2017 in zaak nr. 16/5602;
- IV. vernietigt de einduitspraak van de rechtbank Midden-Nederland van 7 september 2017 in zaak nr. 16/5602;
- V. verklaart het bij de rechtbank ingestelde beroep ongegrond;
- VI. vernietigt het besluit van de minister van Algemene Zaken van 4 december 2017, kenmerk 3972994.

Aldus vastgesteld door mr. C.J. Borman, voorzitter, en mr. E. Steendijk en mr. C.M. Wissels, leden, in tegenwoordigheid van mr. Y. Soffner, griffier.

w.g. Borman w.g. Soffner
voorzitter griffier

Uitgesproken in het openbaar op 16 januari 2019

818.

BIJLAGE

EVRM

Artikel 10

1. Een ieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. Dit artikel belet Staten niet radio- omroep-, bioscoop- of televisieondernemingen te onderwerpen aan een systeem van vergunningen.

2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen.

Grondwet

Artikel 45

1. [...]

2. [...]

3. De ministerraad beraadslaagt en besluit over het algemeen regeringsbeleid en bevordert de eenheid van dat beleid.

Wob

Artikel 1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a. [...]

b. [...]

c. intern beraad: het beraad over een bestuurlijke aangelegenheid binnen een bestuursorgaan, dan wel binnen een kring van bestuursorganen in het kader van de gezamenlijke verantwoordelijkheid voor een bestuurlijke aangelegenheid;

d. [...]

e. [...]

f. persoonlijke beleidsopvatting: een opvatting, voorstel, aanbeveling of conclusie van een of meer personen over een bestuurlijke aangelegenheid en de daartoe door hen aangevoerde argumenten;

g. [...]

Artikel 10

1. [...]

2. Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:

a. de betrekkingen van Nederland met andere staten en met internationale organisaties;

b. [...]

c. [...]

d. [...]

e. [...]

f. [...]

g. het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.

Artikel 11

1. In geval van een verzoek om informatie uit documenten, opgesteld ten behoeve van intern beraad, wordt geen informatie verstrekt over daarin opgenomen persoonlijke beleidsopvattingen.

2. Over persoonlijke beleidsopvattingen kan met het oog op een goede en democratische bestuursvoering informatie worden verstrekt in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.

Reglement van orde voor de ministerraad

Artikel 26

1. Ten aanzien van hetgeen ter vergadering besproken wordt of geschiedt, bestaat een geheimhoudingsplicht.

2. De geheimhoudingsplicht bestaat niet:

a. voor zover de raad of de minister-president namens de raad ontheffing van de geheimhouding verleent;

b. voor zover uitvoering van besluiten dit nodig maakt, dan wel de aard en omstandigheden van een besluit bekendmaking daarvan vorderen.

3. Dit artikel is van overeenkomstige toepassing met betrekking tot de vergaderingen van de onderraden en commissies uit de raad.



Bijlage 9

E-mailbericht informatie staatsgeheim in relatie tot de Wob

From: [...]
To: [...]
Cc: [...]
Subject: Ter info: relatie rubricering-Wob / [...]-Taskforce
Date: donderdag 19 juli 2018 11:17:00

Beste allen,

Ik zou nog informatie aanleveren over de rubricering 'Staatsgeheim' en de betekenis daarvan voor de Wob. De relevante regels zijn opgenomen in de Wet bescherming staatsgeheim en het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).

In de toelichting bij het VIRBI 2013 staat het volgende over de relatie rubricering-Wob: *"Bij een verzoek in het kader van de Wet Openbaarheid Bestuur (Wob) wordt op grond van artikel 5 de rubricering opnieuw beoordeeld. De rubricering van de informatie of delen daarvan moet(en) worden beëindigd als de belangen niet onder de uitzonderingsgronden van de Wob vallen. Informatie die wordt vrijgegeven op basis van een dergelijk verzoek kan immers niet langer gerubriceerd zijn. Indien delen niet worden gederubriceerd, moeten deze onleesbaar worden gemaakt in, dan wel verwijderd uit het vrij te geven document."*

Concreet betekent dit dat een rubricering een invulling kan zijn van een uitzonderingsgrond van de Wob, een invulling van een argument waarom bepaalde informatie/documenten niet openbaar worden gemaakt. Een rubricering is geen afzonderlijke grond in de Wob om informatie/documenten niet openbaar te maken.

Zie hieronder voor meer informatie, waaronder over de criteria voor de inschaling van de rubricering, namelijk 'schade' en 'belang'.

Ik hoor graag indien jullie (vervolg)vragen hebben.

Groet,
[...]

Wet bescherming staatsgeheimen

- In de Wet bescherming staatsgeheimen is aangegeven dat staatsgeheimen gegevens betreffen waarvan de geheimhouding door het belang van de Staat wordt geboden.
- In artikel IIA is opgenomen dat onder de veiligheid van de Staat ook wordt verstaan de veiligheid van diens bondgenoten.
- Informatie waarvan de geheimhouding is geboden door het belang van één of meerdere ministeries en niet als Staatsgeheim is gerubriceerd, wordt als Departementaal Vertrouwelijk gerubriceerd.

Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)

- **Artikel 4 van VIRBI 2013** ziet op de niveaus van rubricering. Uit dat artikel blijkt dat informatie moet worden voorzien van een passend niveau van rubricering, indien geheimhouding van de informatie vanwege het belang van de Staat, zijn bondgenoten of van één of meer ministeries is geboden.

- De volgende rubriceringsniveaus bestaan (waaronder drie niveaus 'staatsgeheim'):
 - a. Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG): indien kennisname door niet geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
 - b. Staatsgeheim GEHEIM (afgekort Stg.G): indien kennisname door niet geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
 - c. Staatsgeheim CONFIDENTIEEL (afgekort Stg.C): indien kennisname door niet geautoriseerden schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
 - d. Departementaal VERTROUWELIJK (afgekort Dep.V.): indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.

- De inschaling van de rubricering wordt (dus) op basis van twee criteria bepaald: schade en belang.

Schade

De mate van schade aan een belang is mede bepalend voor de hoogte van de rubricering. Uitgegaan is van de volgende criteria in oplopende volgorde:

- a. Schade: beperkte nadelige invloed;
- b. Ernstige schade: nadelige invloed, korte termijn geen alternatieven;
- c. Zeer ernstige schade: onmisbaar, geen alternatieven mogelijk.

Belang

De mate van vitaliteit van de belangen voor de Staat of haar bondgenoten of een belang van een of meerdere ministeries is mede bepalend voor de hoogte van de rubricering.

Voor de bepaling van de (vitale) belangen van de Staat en/of haar bondgenoten is aangesloten op de vijf onderscheiden vitale belangen in de Strategie Nationale Veiligheid, die de basis is voor de Rijksbrede aanpak van de nationale veiligheid. Deze vitale belangen zijn als volgt gedefinieerd:

- a. territoriale veiligheid: het ongestoord functioneren van Nederland als onafhankelijke staat, en in het bijzonder de territoriale integriteit van het grondgebied en de internationale positie;
- b. fysieke veiligheid: het ongestoord functioneren van de mens in Nederland en zijn omgeving;
- c. economische veiligheid: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie;
- d. ecologische veiligheid: het beschikken over voldoende zelfherstellend vermogen van de leefomgeving bij aantasting;
- e. sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden.

- **Artikel 5 van VIRBI 2013** ziet op het herzien en beëindigen van een rubricering.
- De geheimhouding van bijzondere informatie is noodzakelijk voor een specifieke periode

of verbonden aan een bepaalde gebeurtenis, maar zal niet automatisch vervallen. De rubricering wordt daarom altijd aangevuld met een maximum tijdsverloop of bepaalde gebeurtenis, na dit tijdsverloop of de bepaalde gebeurtenis dient de noodzaak tot en de hoogte van de rubricering opnieuw te worden vastgesteld. Hiermee wordt enerzijds voorkomen dat informatie onnodig lang beveiligd wordt en anderzijds wordt de geheimhouding van informatie geborgd zolang dit noodzakelijk is.

- **Bij een verzoek in het kader van de Wet Openbaarheid Bestuur (Wob) wordt op grond van artikel 5 de rubricering opnieuw beoordeeld. De rubricering van de informatie of delen daarvan moet(en) worden beëindigd als de belangen niet onder de uitzonderingsgronden van de Wob vallen. Informatie die wordt vrijgegeven op basis van een dergelijk verzoek kan immers niet langer gerubriceerd zijn. Indien delen niet worden gederubriceerd, moeten deze onleesbaar worden gemaakt in, dan wel verwijderd uit het vrij te geven document.**



Bijlage 10

e-mail bericht bijeenkomst taakgroep verdeling Wob-verzoeken

From: [...]

Sent: donderdag 5 juli 2018 14:07

To: [...]

Subject: Verslag aftrap WOB-Taskforce

Allen,

Bedankt voor jullie aanwezigheid bij de aftrap van de [...]-taskforce. Hierbij een kort verslag met de taakverdeling

[...]

Verdeling WOB-verzoeken

- ☒ WOB AJACS: DSH & DAM in de lead, i.s.m. [...] van IST-SYR.
- ☒ WOB Ambtsberichten SYR: CAT
- ☒ WOB *Fact-finding missie*: DVB in de lead i.s.m. DAM, DSH & [...].
- ☒ WOB Alle gematigde strijdgroepen: IST-SYR & DAM
- ☒ WOB *Jaish al Fatah*: IST-SYR & DAM
- ☒ WOB SRTF: DSH [...] en IST [...]
- ☒ WOB NLA: IST-SYR & DAM in de lead, i.s.m. DVB & DSH