Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 AE Den Haag

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2018-0000814684

Uw kenmerk

Datum 11 oktober 2018
Betreft Sturing informatiebeveiliging en ICT binnen de Rijksdienst

De samenleving is in hoge mate afhankelijk van diensten van de Rijksoverheid. Die diensten zijn en worden in toenemende mate digitaal georganiseerd. Over de ambitie van het kabinet ten aanzien van de digitalisering van onze samenleving en van de overheid heeft het kabinet uw Kamer onlangs de Nederlandse Digitaliseringsstrategie[1] en de Agenda Digitale Overheid[2] gestuurd. Het kabinet is van mening dat wij in het licht van de digitale ontwikkelingen in de samenleving en de overheid onze inzet op alle fronten verder moeten versterken. Voor digitalisering binnen de Rijksoverheid vertaalt dit zich, in het verlengde van de Agenda Digitale Overheid, naar scherpere en meer eenduidige sturing op de volgende terreinen:

- *Informatiebeveiliging.* Wij constateren dat de Rijksoverheid, net als alle andere organisaties en individuen, kwetsbaarder wordt voor de snel toenemende hoeveelheid en van aard veranderende cyberaanvallen. Met name ten aanzien van de bescherming van gegevens van burgers en bedrijven mag van de Rijksoverheid juist een hoge mate van zorgvuldigheid worden verwacht. De plicht die zij oplegt aan burgers en bedrijven tot het verstrekken van gegevens onderstreept de hoge eisen die terecht aan haar worden gesteld. De Algemene Rekenkamer constateerde over het jaar 2017 negen onvolkomenheden in de informatiebeveiliging bij de departementen[3]. Dit noodzaakt de Rijksdienst om in gezamenlijkheid hierop te gaan sturen;

- *Informatiehuishouding en openbaarheid.* In een wereld waar feiten en meningen in het digitale domein moeilijk van elkaar onderscheiden kunnen worden, ligt ook een zware verantwoordelijkheid voor de overheid om betrouwbaarheid en volledigheid van overheidsinformatie te waarborgen; een solide en toegankelijke informatiehuishouding is hiervoor onmisbaar.

- *ICT-ontwikkeling en beheer.* Omdat digitalisering een rol speelt in vrijwel alle uitvoeringsprocessen en raakt aan vrijwel alle nieuwe beleid, is grip op ICT-

[1] *Nederlandse Digitaliseringsstrategie, Nederland Digitaal*, bijlage bij *Kamerstukken II* 2017/18, 26643, 541
[2] *NL Digibeter, Agenda Digitale Overheid*, bijlage bij *Kamerstukken II* 2017/18, 26643, 549
[3] Bijlage bij *Kamerstukken II* 2017/18, 34950-XVIII, 2

projecten en het ICT-landschap randvoorwaardelijk voor de uitvoering van deze en andere maatschappelijke opgaven. Afgelopen jaren is op basis van de maatregelen uit het eindrapport van de commissie Elias[4] met mijn collega's samengewerkt en zijn er resultaten geboekt, zoals de verdere inrichting het van CIO stelsel bij de Rijksdienst en de oprichting van het Bureau ICT-Toetsing (BIT)[5]. Ik constateer in navolging van uw Kamer[6] dat de realisatie van deze digitaliseringsopgave versterking behoeft. Initiatieven zoals het BIT en gateway reviews dragen ontegenzeggelijk bij aan de beheersbaarheid, maar we zijn er nog niet.

De minister van Financiën zegde bij het Verantwoordingsdebat 2017 toe[7] dat ik uw Kamer na de zomer een brief zou sturen met heel concrete nieuwe voorstellen rondom ICT en informatiebeveiliging. Het verantwoordingsonderzoek van de Algemene Rekenkamer over 2017 had, zoals gezegd, bij 9 ministeries een onvolkomenheid op het gebied van informatiebeveiliging geconstateerd. De president van de Rekenkamer merkte op Verantwoordingsdag op dat hij verwachtte dat in een tijd waarin digitale criminaliteit, digitale spionage en cyberoorlog een reëel risico zijn, informatiebeveiliging hoog op de politieke agenda staat[8]. De Rekenkamer adviseerde om de taak van de minister van BZK nader te bezien[9]. Ik heb de toezegging van mijn collega van Financiën herhaald bij het Algemeen Overleg Functioneren Rijksdienst[10] waar mijn brief[11] van 22 december 2017 stond geagendeerd in het antwoord op de motie de Vries[12]. Ik heb in dat AO tevens toegezegd in deze brief in te gaan op de sturing op ICT binnen de Rijksdienst naar aanleiding van in uw Kamer geuite zorgen over dit onderwerp[13,14]. In deze brief adresseer ik mijn beleidsvoornemens en initiatieven voor deze onderwerpen.[15]

Voor de voorgenoemde drie beleidsterreinen zal ik allereerst de concrete maatregelen schetsen die het kabinet op korte termijn nodig acht. Daarna ga ik in op de coördinatiemiddelen die daarvoor nodig zijn. De verwevenheid van ICT in vrijwel alle departementale processen maakt dat de primaire verantwoordelijkheid voor de digitaliseringsopgave binnen de verschillende beleidsterreinen van de Rijksoverheid belegd moet zijn bij de individuele vakministers. Dit uitgangspunt

[4] *Grip op ICT*, *Kamerstukken II* 2014/15, 33326, 5
[5] *Kamerstukken II* 2016/17, 26433, 454
[6] *Handelingen II,* 2017/18, 84, item 3
[7] *Handelingen II,* 2017/18, 84, item 6, p. 15
[8] Toespraak van de directeur van Algemene Rekenkamer, 16 mei 2018, rekenkamer.nl
[9] Bijlage bij *Kamerstukken II* 2017/18, 34950-XVIII, 2
[10] *Kamerstukken II* 2017/18, 31490, 241
[11] *Kamerstukken II* 2017/18, 34775 VII, 47
[12] *Kamerstukken II* 2016/17, 34725, 5
[13] *Handelingen II,* 2017/18, 101, item 2
[14] *Handelingen II,* 2017/18, 34 950, VII, nr. 7
[15] De staatssecretaris van BZK zal u ook, zoals door hem toegezegd in de Agenda Digitale Overheid, in het najaar een brief doen toekomen over zijn voornemens voor versterking van de informatieveiligheid in het kader van digitale overheidsdienstverlening voor alle overheidslagen.

vloeit ook voort uit artikel 44 van de Grondwet en is verankerd in verschillende regelingen, onder andere in het Besluit informatievoorziening in de Rijksdienst 1990 (IVR 1990)[16]. Tegelijkertijd is het kabinet van mening dat de maatregelen in deze brief beter en effectiever in gezamenlijkheid kunnen worden opgepakt. Dit betekent niet dat meer control en rapportage het uitgangspunt zijn, maar we moeten elkaar wel kunnen aanspreken als we op basis van feitelijke informatie constateren dat zaken beter kunnen. Ik zal hier binnen de Rijksdienst graag een voortrekkersrol in spelen, in het verlengde van de overheidsbrede aanpak van de staatssecretaris van BZK. Daarom stuur ik deze brief ook mede namens hem.

Informatiebeveiliging
Naast de aandacht en zorg van individuele departementen voor informatiebeveiliging slaagt de huidige opgave voor informatiebeveiliging alleen met een aantal gezamenlijke elementen. Een aantal van dergelijke elementen bestaat al, zoals GovCERT (opgegaan in het Nationaal Cyber Security Centrum, NCSC), de Baseline Informatiebeveiliging Rijksdienst (BIR) en de Audit Dienst Rijk[17]. Deling van kennis, interdepartementaal, helpt om risicomanagement departementaal beter in te richten.

Technologische ontwikkelingen en de toename van digitale dreigingen vragen echter voortdurend om nieuwe aanvullende elementen. De overheid moet hier het goede voorbeeld geven en treedt als launching costumer op. Mijn collega van J&V is hier volop mee bezig vanuit zijn coördinerende rol op het gebied van cybersecurity zoals blijkt uit de onlangs verschenen Nederlandse Strategische Cybersecurity Agenda[18]. Ook werken hij en ik intensief samen met de andere collega's in het recente opgericht SIB, het Strategische Informatiebeveiligingsberaad van de Rijksdienst.

De volgende initiatieven zijn thans actueel, dragen bij aan de feitelijke weerbaarheid en zijn onder andere het resultaat van een eerste verkenning naar centrale voorzieningen, zoals aangekondigd in mijn bestuurlijke reactie op het conceptrapport de Staat van de Rijksverantwoording 2017[19]:

- *Implementatie centrale voorziening: vulnerability scanning.*
  Ontwikkeling en inrichting van een gezamenlijke faciliteit voor vulnerability scanning. Dat wil zeggen: het geautomatiseerd controleren van alle systemen van de Rijksdienst die met het internet zijn verbonden op bekende kwetsbaarheden. Ook dit is een kennisintensief terrein, dat gemakkelijker gezamenlijk kan worden opgepakt. Ook biedt gezamenlijke inrichting het voordeel dat vergelijkingen (benchmarks) mogelijk worden en departementen gerichter en beter van elkaar kunnen leren;

[16] *Stcrt.* 1991, 20
[17] Ten behoeve van rijksbrede informatiebeveiligingsonderzoeken.
[18] Zie onder meer *Nederlandse Cybersecurity Agenda, Nederland digitaal veilig*, bijlage bij *Kamerstukken II* 2017/18, 26643, 536
[19] Brief aan de president van de Algemene Rekenkamer, met kenmerk 2018-0000246317

- *Uitbouw van het Nationaal Detectie Netwerk[20] (NDN) bij de Rijksdienst.* Het NDN is steeds effectiever bij een toenemende graad van aansluitingen. In april 2014 is bij de Rijksdienst een succesvolle pilot gestart met een looptijd van zes maanden. De Rijksdienst fungeerde toen als *launching customer*; het belang van deze rol wordt ook benadrukt in de Nationale Cybersecurity Agenda. Tot op heden zijn er op basis van vrijwilligheid een beperkt aantal rijksoverheidspartijen op het NDN aangesloten. In het licht van de toenemende digitale dreigingen en dus de urgentie van deze maatregel voor een goede informatiebeveiliging binnen de Rijksdienst hebben de ministeries afspraken gemaakt over een versnelde uitbouw van het NDN bij de Rijksdienst;

- *Opstellen van een lijst van vereiste beveiligingsmaatregelen.*
  Ondanks dat ministeries onderling verschillen, is er een aantal concrete beveiligingsmaatregelen te bedenken, die interdepartementale geldigheid hebben en waarvan de aanwezigheid ook geverifieerd kan worden. Deze lijst beveiligingsmaatregelen zal samen met de departementen opgebouwd worden en aanvullend op de BIR zijn. Waar de BIR vooral maatregelen op bestuurlijk niveau voorschrijft, zal deze lijst meer tactisch/operationeel van karakter zijn en systeemvereisten vastleggen die departementen helpen en richting geven bij de ontwikkeling of acquisitie van systemen. Ik denk bijvoorbeeld aan de toepassing van zogenaamde Security Technical Implementation Guides (STIGs) die een belangrijke aanvulling zijn op de Baseline Informatiebeveiliging Rijksdienst, omdat die invulling geven op systeemniveau voor de te treffen maatregelen. Een aantal onderdelen van de Rijksdienst heeft hiermee positieve ervaringen opgedaan.

- *Staatsgeheime werkplek*
  Ook de beveiliging van de eigen gegevens van de overheid moet goed zijn. Dat geldt voor de gegevens die standaard als vertrouwelijk worden beschermd, en des te meer nog voor staatsgeheimen. Gezien de toegenomen dreigingen (mede door statelijke actoren) en de schaarse kennis die nodig is om voorzieningen te ontwikkelen en te accrediteren die deze dreigingen kunnen weerstaan, heb ik het voornemen het gezamenlijk kader voor een voorziening voor staatsgeheime toepassingen te ontwikkelen. Op basis van een dergelijk kader zal ik een onderzoek doen naar een gezamenlijke voorziening, die recht doet aan de specifieke eisen van departementen en internationale eisen zodat deze voorziening zo breed mogelijk binnen de Rijksdienst kan worden ingezet.

Informatiehuishouding en openbaarheid van bestuur
Een solide en toegankelijke informatiehuishouding is een essentiële randvoorwaarde om een snellere, laagdrempeliger en betere toegang van burgers en bedrijven tot overheidsinformatie mogelijk te maken. Actieve openbaarmaking

[20] Het Nationaal Detectie Netwerk is een door het Nationaal Cyber Security Centrum gestart initiatief om, samen met de inlichtingen- en veiligheidsdiensten, aanvallen van buitenaf sneller te detecteren en informatie over deze en andere dreigingen sneller te delen binnen de Rijksoverheid (Threat Intel Platform).

van overheidsinformatie is van groot belang voor de controleerbaarheid van de overheid en de herbruikbaarheid van overheidsinformatie door burgers en bedrijven.

Op dit terrein moet nog veel gebeuren, ook in de ICT c.q. de systemen waarin deze informatie is opgeslagen. Daarnaast vormt de door mijn collega van OCW aangekondigde verkorting van de overbrengingstermijn onder de Archiefwet[21] een aanleiding om meer werk te maken van de (digitale) informatiehuishouding. Te denken valt bijvoorbeeld aan het beter beschikbaar en vindbaar maken van de ARVODI-rapporten[22] en (externe) onderzoeksrapporten. Daarnaast wordt momenteel hard gewerkt om de duurzame toegankelijkheid en archivering van e-mails en websites te borgen.

Ook hier ligt de primaire verantwoordelijkheid bij de individuele departementen. Niettemin verwacht het kabinet dat met een beperkt aantal gezamenlijke voorzieningen en kaders een versnelling kan worden bereikt en een grotere consistentie voor burgers.

Ontwikkeling en beheer van Informatievoorziening en ICT
Betere en snellere digitalisering vereist meer beheerste aanpassingen van het ICT-landschap dan nu het geval is, in kleinere stappen. Dit levert sneller resultaten, en creëert daarmee meer flexibiliteit voor veranderingen onderweg. Ook is de Rijksoverheid gebaat bij integrale borging van expertise en (mede)sturing vanuit het I-domein, in alle fasen van beleid en uitvoering. Vanuit deze ervaringen gaan we de volgende maatregelen in overleg met de departementen verder invullen:

- *Definiëren en versterken van de positie van de departementale CIO.* De traditionele invulling van de CIO-rol plaatst diens expertise controlerend op een zekere afstand. In veel departementen heeft de CIO al een ruimere rol gekregen, eerder in het proces (dat wil zeggen: al in de fase van beleidsvorming en de definitie van grote projecten) en intensief samenwerkend met "de lijn", dat wil zeggen de verantwoordelijke beleids- en uitvoeringsdirecties en -directoraten generaal. Ik zie echter nog ruimte om de rol en het mandaat van de CIO nog consequenter in te vullen en te versterken ten aanzien van het opstellen en onderhouden van het departementale informatieplan. In de zienswijze van het kabinet is de departementale CIO degene die in opdracht van de bestuursraad bevordert dat het door het departement ontwikkelde beleid in de informatievoorziening uitvoerbaar is, dat het nieuwe beleid adequaat in de informatievoorziening wordt geïmplementeerd, en dat tegelijkertijd voldoende aandacht uitgaat naar continue verbetering van het bestaande systeemlandschap, inclusief de benodigde technologische vernieuwing. Vaak dient de CIO hierbij ook rekening te houden met belangen en systemen van partijen buiten het Rijk en voor hen regels op te stellen of daarover minstens te adviseren. De CIO

[21] *Kamerstukken II* 2016/17, 29362, 272
[22] Rapporten waarvoor een ministerie aan andere organisaties opdracht heeft gegeven onder de Algemene Rijksinkoopvoorwaarden (ARVODI).

bevordert daarmee het ICT-belang in het primaire proces, zowel vroeg in de begrotings- en beleidscyclus maar ook in de stadia van beheer en doorontwikkeling ná oplevering van ICT-projecten. Het leeuwendeel van de ICT-kosten binnen de Rijksoverheid is immers met laatstgenoemde aspecten gemoeid.[23]

- *Definiëren van een kwaliteitskader waarbij we doorontwikkelen naar kwaliteitseisen voor departementale I-plannen.*
  Het is van belang de sturing op informatie en ICT te integreren in de begrotings- en beleidscyclus van de departementen via de I-plannen. Elementen voor zo'n kader kunnen zijn een analyse van het bestaande applicatielandschap, een inventarisatie van het benodigde onderhoud en technische vernieuwing, een overzicht van de gewenste vernieuwing op basis van beleid, en een samenvattend overzicht van daaruit resulterende projectportfolio en onderhoudsplan en de daarvoor benodigde middelen. Deze elementen krijgen een plaats in het departementale I-plan. De departentale CIO is verantwoordelijk voor de totstandkoming van dit overall I-plan, waarbij uiteraard de eindverantwoordelijkheid voor projecten en beheer bij de lijnorganisatie blijft. Door op basis van rijksbrede best practices, BIT adviezen en lessons learned uit grote ICT-projecten kwaliteitseisen te stellen, ontstaat zo een beter zicht op de consequenties van beleid voor het gehele bestaande ICT en gegevenslandschap. Dit faciliteert goed opdrachtgeverschap, een goede beheersing van ICT-ontwikkeling en -onderhoud, alsook de aansluiting van de departementale informatieplanning op de begrotings- en beleidscyclus. Ik verwacht dat dit kwaliteitskader onder meer de schattingskwaliteit en verantwoording van kosten en doorlooptijd van ICT-projecten, waar uw Kamer recent nog de nodige vragen over stelde[24], ten goede zal komen.

- *Bevordering van de interoperabiliteit van systemen bij verschillende Rijksdienstonderdelen en toezien op naleving daarvan.*
  Het is door de grote diversiteit van het ICT-landschap binnen de Rijksoverheid momenteel een uitdaging om systemen optimaal te laten samenwerken. Inrichtingseisen voor interoperabiliteit (bijvoorbeeld de zogeheten IDWOR[25]-standaarden) zijn nodig. Daarbij wordt aangesloten op de interoperabiliteitsafspraken die per sector gelden, of die in internationaal verband (bv de NAVO) worden gemaakt; deze prevaleren immers.

- *Sourcing strategie.*
  Het landschap van ICT-dienstverleners binnen het Rijk is de afgelopen jaren gegroeid en tamelijk ingewikkeld geworden. Vereenvoudiging is mogelijk en nodig. Ik streef naar het opstellen van een sourcing strategie voor de

[23] Jaarrapportage Bedrijfsvoering Rijk 2017, bijlage bij *Kamerstukken II* 2017/18, 31490, 239

[24] *Aanhangsel Handelingen II*, 2017/18, 3209

[25] IDWOR staat voor Interoperabiliteitskader voor Digitale Werkomgevingen in de Rijksdienst. Dit kader draagt ervoor zorg dat ambtenaren over de grenzen van hun departement heen makkelijker met elkaar kunnen samenwerken, bijvoorbeeld door middel van het delen van agenda's en video-conferencing.

Rijksdienst, waar ik het gebruik van (standaard)producten en diensten uit de markt wil bevorderen, waaronder de mogelijkheid om afgewogen gebruik te maken van producten en diensten uit de zogenaamde *public cloud*. Dan zal ook bezien worden wat dit betekent voor het interne landschap van ICT-dienstverleners.

Benodigde coördinatie en sturing
De snelheid en effectiviteit waarmee voorgenoemde maatregelen op basis van bestaande afspraken kunnen worden gerealiseerd, is beperkt. In de strategische I-agenda Rijksdienst zullen we na overleg met de departementen de bovenstaande inhoudelijke en organisatorische interventies vastleggen. Zo ontstaat een stevige ontwikkelagenda voor de sturing op de Rijksdienst.
Daarnaast heeft het kabinet besloten de minister van BZK een aantal gerichte instrumenten toe te kennen op bovenstaande terreinen, met inachtneming van het uitgangspunt van de individuele ministeriële verantwoordelijkheid zoals vastgelegd in artikel 44 van de Grondwet. Deze instrumenten hebben onder meer betrekking op:

- de mogelijkheid om na overleg met mijn collega's afgewogen rijksbrede kaders te kunnen stellen op voorgenoemde terreinen. Die kaders kunnen ook gaan over gebruikmaken van een gezamenlijke voorziening die de informatiebeveiliging, openbaarheid of interoperabiliteit bevordert. Ten aanzien van de deelname aan een aangewezen voorziening wordt uiteraard rekening gehouden met de omstandigheden en benodigdheden in de onderscheiden ministeries. Bij de vaststelling van de kaders zullen conform de begrotingsregels de budgettaire gevolgen worden meegenomen;
- het recht om informatie van andere ministeries te ontvangen ten behoeve van monitoring van de gestelde kaders, waarbij rekening wordt gehouden met de beheerslast voor de ministeries en de deelbaarheid van staatsgeheime informatie.

Uw Kamer suggereerde in dit verband de afgelopen jaren meerdere malen, meest recent nog bij het Verantwoordingsdebat 2017, om de bevoegdheden en verantwoordelijkheden van de minister van BZK op een vergelijkbare wijze in te vullen als die van de minister van Financiën rond de rijksfinanciën[26,27].
Ik laat me graag inspireren door het financiële sturingsmodel voor het ICT-domein inclusief de informatiehuishouding. Daarbij merk ik wel op dat inhoudelijk financiën en ICT echt twee verschillende domeinen zijn, en de analogie ook zijn beperkingen kent.

Het kabinet herziet het Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst 2011[28] om invulling te geven aan deze brief. Ook de Commissie Elias wees destijds in haar beschouwing op de noodzaak om ten behoeve van coördinatie en systeemverantwoordelijkheid meer te doen[29]. Om het belang van

[26] *Kamerstukken II* 2016/17, 31490, 227 en 2017/18, 34775 VII, 12 (motie Middendorp-Van der Molen)
[27] *Handelingen II* 2017/18, 84, item 3, p.4
[28] *Stb.* 2011, 18
[29] *Handelingen II* 2014/15, 36, item 9, p.21

informatievoorziening en ICT te benadrukken wijzigt ook de titel van het besluit in "Coördinatiebesluit organisatie, bedrijfsvoering *en informatiesystemen* rijksdienst" (bijlage). Het nieuwe besluit bevat ook een adviesrecht van de minister van BZK bij benoeming en ontslag van departementale CIO's.

Bij al het voorgaande zullen we moeten voorkomen dat er een controletoren of verantwoordingscircus ontstaat. Het gaat om transparantie en elkaar aanspreken waarbij het ministerie van BZK de voortrekkersrol vervult.

Ik realiseer mij dat voor voorgenoemde beleidsmaatregelen niet alleen een vernieuwde governance maar ook aanvullende middelen, in de vorm van personele capaciteit en geld, nodig zijn. Ik streef ernaar dit binnen de begroting van het ministerie van BZK op te lossen.

Tot slot
De in deze brief genoemde beleids- en uitvoeringsmaatregelen zijn niet uitputtend maar vormen een samenhangend geheel met initiatieven die minder afhankelijk zijn van versterking van regie en bevoegdheden, zoals de Rijksacademie voor Digitalisering en Informatisering Overheid (RADIO) en het Plan van Aanpak Versterking HR ICT Rijksdienst[30] ten aanzien van werving van specialisten en kennis en kunde binnen de Rijksoverheid. Het ministerie van BZK vervult hier de rol van aanjager, verbinder en platform voor kennisdeling.

Het is onze overtuiging dat de combinatie van deze inhoudelijke, organisatorische en bestuurlijke maatregelen de informatieveiligheid, de openbaarheid en uitvoering van ICT-projecten zal verbeteren. In de strategische I-agenda, die ik na het kerstreces naar uw Kamer zal zenden, zullen alle maatregelen in samenhang beschouwd worden.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. K. H. Ollongren

[30] *Kamerstukken II* 2017/18, 31490, 235