

**35830-V Rapport van de Algemene Rekenkamer: Resultaten
verantwoordingsonderzoek 2020 bij het Ministerie van Buitenlandse
Zaken**

nr. Lijst van vragen en antwoorden

Vastgesteld (*wordt door griffie ingevuld als antwoorden er zijn*)

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen voorgelegd aan de minister van Buitenlandse Zaken over het rapport *Resultaten verantwoordingsonderzoek 2020 bij het Ministerie van Buitenlandse Zaken* van de Algemene Rekenkamer (Kamerstuk 35 830-V, nr. 2).

De daarop door de minister gegeven antwoorden zijn hierbij afgedrukt.

Fungerend voorzitter van de commissie,
Wilders

Adjunct-griffier van de commissie,
Konings

Nr	Vraag	Bijlage	Blz. (van)	t/m
1	Waarom kost het uitbreiden van het aanbod aan theesmaakjes op het ministerie 75.000 euro? Hoeveel extra theesmaakjes kan je met dit bedrag kopen?		0	

Antwoord:

Voor de renovatie, het onderhoud en exploitatie van de Rijnstraat 8 (R8) is destijds door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en het Ministerie van Financiën gekozen voor een zgn. Publiek Private Samenwerking (PPS) constructie. Dat is een langlopend contract van 25 jaar. Het (financieel) beheer ligt bij het BZK en het Rijksvastgoedbedrijf als eigenaar van het DBFMO-contract met het consortium. Het Ministerie van Buitenlandse Zaken is samen met I&W, IND, COA en DT&V gebruiker van R8. Het betreft een uitbreiding met vijf smaken. Daarmee is het aanbod in lijn gebracht met wat in andere Rijkskantoren gangbaar is. Voor verdere details moet ik doorverwijzen naar BZK.

- 2 Op welk moment is begonnen met het vaccineren van uitgezonden en lokale medewerkers in hoog-risicogebieden? Hoeveel medewerkers van het ministerie van Buitenlandse Zaken (uitgezonden en lokaal) zijn in het buitenland aan corona gestorven?

Antwoord:

Vaccinatie van ambassademedewerkers en civiel experts in landen waar (voorlopig) geen EMA-goedgekeurde vaccins beschikbaar zijn en de medische voorzieningen in veel gevallen gebrekkig, is op 5 mei jl. gestart. In het afgelopen jaar zijn er verschillende collega's gestorven. Het ministerie van Buitenlandse Zaken heeft als werkgever echter geen toegang tot het medisch dossier van een werknemer. Er wordt geen registratie bijgehouden van de doodsoorzaak.

- 3 Wanneer was het eerste bericht in het Buitenlandse Zaken-berichtenverkeer dat melding maakte van corona-ziekte in China?

Antwoord:

In het officiële BZ berichtenverkeer dateert het eerste bericht van 28/1/20, dat betreft een bericht van de personeelsafdeling aan het postennetwerk in China over o.a. in acht te nemen hygiënemaatregelen n.a.v. het nieuwe Coronavirus. Informatie wordt overigens veelal ook gedeeld via interne email-correspondentie. Het Corona-virus kwam daarin voor het eerst ter sprake op 6/1 in correspondentie tussen het postennetwerk China en Den Haag n.a.v. nieuwsberichten over een nieuwe longziekte in Wuhan.

- 4 Kunt u de problemen met de afscherming van de persoonsgegevens van reizigers in de systemen van het ministerie van Buitenlandse Zaken verder toelichten? 5

Antwoord:

De betreffende dossiers waren opgeslagen in een systeem dat was ingericht op basis van het 'Open, tenzij'-principe. Bij het aanmaken van een dossier in dat systeem moet worden gecontroleerd of de aard van de informatie in het dossier afscherming vereist. Als dat vanwege privacy of informatiebeveiliging het geval is, kan de toegang tot het dossier worden beperkt tot specifiek geautoriseerde medewerkers. Dat had in dit geval van de persoonsgegevens van reizigers moeten gebeuren, maar is niet gebeurd. Daardoor waren de dossiers toegankelijk voor iedere medewerker met een BZ-account. Inmiddels is besloten, mede op advies van de ARK, om systemen niet langer 'open, tenzij' in te richten, maar 'gesloten, tenzij': de toegang wordt alleen verleend op basis van *need to know*.

- 5 Betreffende de gevallen waardoor de tolerantiegrens van afgerekende voorschotten is overschreden: op welke zaken hadden deze voorschotten betrekking? Vanuit welke afdeling(en) van het departement werden deze voorschotten geaccordeerd? Op welke begunstigde(n) hadden deze voorschotten betrekking? 11

Antwoord:

Drie gevallen hebben veroorzaakt dat de tolerantiegrenzen zijn overschreden. Bij twee activiteiten is het voorschot afgeboekt terwijl de inhoudelijke voortgangsrapportage nog niet was geleverd. Bij de derde activiteit bestond nog onzekerheid over het exacte Nederlandse aandeel. Deze voorschotten zijn gecorrigeerd en afboeking vindt alsnog plaats wanneer er voldoende verantwoordingsinformatie is.

Het afboeken van een voorschot betreft een interne jaarlijkse administratieve bijstelling. Dit wil niet zeggen dat er middelen oneigenlijk zijn besteed.

Deze fout is intern gemaakt bij de decentrale control-afdeling. Dat lag niet aan de ontvangende partijen zoals UNDP, *Global Center on Cooperative Security* en de *Danish Demining Group*.

- 6 Betreffende de geconstateerde fout waarbij de liquiditeitsbehoefte van de ontvangende partij de betaling niet rechtvaardigde: bij welke afdeling van het departement en op welke wijze kon deze fout plaatsvinden? Wie was de ontvangende partij? Is de betaling teruggedraaid? Zo nee, waarom niet? 12

Antwoord:

In de subsidiebeschikking waar deze betaling betrekking op had, was opgenomen dat in januari 2021 zou worden betaald op basis van een liquiditeitsverzoek. De betaling heeft echter plaatsgevonden in december 2020 en is hiermee in het verkeerde verantwoordingsjaar verricht. In 2021 worden met deze betaling de beleidsresultaten uit deze financiering gerealiseerd. Om deze reden heeft geen correctie van de betaling plaatsgevonden.

Deze fout is intern gemaakt bij de decentrale control-afdeling. Dat lag niet aan de ontvangende partij *Netherlands Helsinki Committee*.

- 7 Wordt er Rijksbreed nagedacht over hoe het werken post-corona wordt vormgegeven? 13

Antwoord:

Ja, er is een rijksbrede discussie over de toekomst van het zogeheten *hybride werken*, dat tevens een gelijknamig programma vormt binnen de rijksbrede ambitie om in 2022 tot een meer wendbare rijksdienst te komen die 'bewust en grenzeloos samenwerkt'. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties coördineert dit rijksbrede programma en afstemming vindt plaats in de Interdepartementale Commissie Huisvesting en Faciliteiten (ICHF) en de Interdepartementale Commissie Bedrijfsvoering Rijksdienst (ICBR).

- 8 Bent u van mening dat met de huidige staat van de accreditaties, het ministerie voldoende veilig kan werken? 15

Antwoord:

Het ministerie heeft de voorwaarden voorlopig ingevuld om veilig met de informatiesystemen te kunnen werken. Er wordt hard gewerkt aan het afronden van de nog openstaande actiepunten en het structureel borgen en monitoren van informatiebeveiliging binnen de organisatie.

- 9 Wat wordt er op dit moment gedaan op het ministerie om cyberaanvallen te voorkomen en af te weren? Is dit voldoende? 15

Antwoord:

Het ministerie werkt nauw samen met diverse organisaties binnen de Rijksoverheid om zich te beschermen tegen cyberaanvallen. Reeds voor de uitbraak van COVID-19 is het ministerie gestart met de uitbreiding van de monitoring capaciteit.

Gezien de snelle ontwikkelingen op dit gebied zal de cyber-weerbaarheid structureel hoge prioriteit moeten krijgen.

- 10 Zijn er gevallen van cyberaanvallen op het ministerie bekend? 15

Antwoord:

Ja, er zijn gevallen van pogingen tot cyberaanvallen bekend. Het ministerie doet hier gezien de vertrouwelijkheid verder geen nadere uitspraken over.

- 11 Hoe werd er omgegaan met het inzicht dat ambtenaren in de thuiswerksituatie de ICT op een risicovolle manier gebruiken, zoals het delen van betrouwbare informatie via WhatsApp? Welke stappen zijn er genomen om dit in het vervolg te voorkomen? 15

Antwoord:

Het ministerie geeft prioriteit aan het duurzaam en veilig omgaan van medewerkers met informatiebeveiliging en privacy. Juist ook in de tijd van het thuis- en online werken.

Gezien de aard van de wereldwijde werkzaamheden van het ministerie was het voor medewerkers van het ministerie voor de uitbraak van COVID-19 al mogelijk om op een veilige manier plaats-onafhankelijk te werken. Bij in gebruik nemen van de mobiele werkplek volgen medewerkers een verplichte training over informatieveiligheid, met aandacht voor het (on)veilig gebruik van ICT-middelen; medewerkers worden er o.a. op geattendeerd voor werk gerelateerde zaken door het ministerie goedgekeurde applicaties te gebruiken. Daarbij wordt ook aandacht besteed aan de risico's van het gebruik van publieke (gratis) applicaties, zoals WhatsApp. In 2020 (tijdens de pandemie) zijn meerdere berichten gepubliceerd op het interne portaal van het ministerie om medewerkers te waarschuwen over de risico's van het verkeerd gebruiken van WhatsApp. Daarnaast wordt dit onderwerp ook actief in trainingen en *e-learning*s behandeld.

- 12 Kan het werken met 'gesloten, tenzij' gevolgen hebben voor de effectiviteit en efficiëntie van het werk van ambtenaren? 17

Antwoord:

Het is belangrijk dat ambtenaren zich bewust zijn van de eventuele gevoeligheid van informatie. Bij het 'open, tenzij' beleid waren de dossiers automatisch voor alle BZ-ambtenaren toegankelijk. Er was actie nodig om af te sluiten en als dat werd verzuimd, stond het dossier dus open. Bij het 'gesloten, tenzij' beleid draaien we dat om. Het dwingt de gebruikers van de systemen om actief toegang te geven aan anderen die met de betreffende informatie moeten werken. Als dat niet gebeurt, dan is er geen risico, want dan staat het dossier dicht. Het 'gesloten

tenzij' zal naar verwachting geen effect hebben, maar vraagt wel een omslag van de medewerkers. In de eerste weken van de implementatie wordt hier extra aandacht aan besteed.

- 13 Wat is het plan van aanpak om bij de toegangsbeveiliging van informatie over te stappen van het 'open, tenzij'-beleid naar het 'gesloten, tenzij'-beleid? Op welke termijn zal deze overstap zijn voltooid? 17

Antwoord:

De implementatie van het 'gesloten, tenzij'-beleid is voor het primaire documentmanagement- en samenwerkingssysteem reeds ter hand genomen. De voltooiing van deze nieuwe inrichting is voorzien voor half juli.

- 14 Wat heeft u gedaan met het datalek van 18.000 personen die tijdens de coronacrisis gerepatrieerd zijn? 17

Antwoord:

Lijsten met reizigersgegevens op de BZ-interne samenwerkingsruimte bleken onvoldoende te zijn afgeschermd. Naast de ambtenaren die vanwege hun functie met de gegevens moesten werken, konden ook andere ambtenaren met een BZ-account bij de gegevens komen. Na melding hiervan door de Algemene Rekenkamer (AR) heeft BZ de betreffende lijsten afgeschermd en een melding van een mogelijk 'datalek' bij de Autoriteit Persoonsgegevens ('AP') gedaan. Intern onderzoek naar de loggegevens wees uit dat er in de periode waarop de lijsten op de samenwerkingsruimte stonden er geen ongeautoriseerde toegang door BZ medewerkers was tot de persoonsgegevens van de reizigers, m.u.v. de betreffende AR medewerker die de melding had gedaan. Hierop is de melding bij de AP weer ingetrokken.

- 15 Hoe schat u de schade in van het datalek? 17

Antwoord:

De betreffende persoonsgegevens stonden op een interne samenwerkingsruimte die alleen toegankelijk was voor medewerkers met een BZ-account. Uit een onderzoek naar de loggegevens blijkt dat alleen een kleine groep bevoegden met een BZ-account en een medewerker van de Algemene Rekenkamer met een BZ-account daadwerkelijk toegang hebben gehad tot de gegevens. Hierom is er geen reden om aan te nemen dat de inbreuk een risico inhoudt voor de betrokkenen. Aangezien er geen sprake was van een meldingswaardig datalek is de melding die gedaan is bij de Autoriteit Persoonsgegevens ('AP') ingetrokken.

- 16 Heeft het ministerie een voldoende plan om datalekken van persoonsgegevens in het vervolg te voorkomen? 18

Antwoord:

Het ministerie heeft extra maatregelen genomen om de kans op een datalek zo klein mogelijk te maken. Zo neemt het ministerie het advies over van de AR om het staande beleid ten aanzien van toegangsbeveiliging van informatie te wijzigen naar 'gesloten tenzij'. Deze beleidswijziging, die al eerder was voorzien, wordt versneld geïmplementeerd.

Het veilig en verantwoord omgaan met persoonsgegevens is van cruciaal belang voor het ministerie. Risicoanalyses op persoonsgegevens maken een vast onderdeel uit van de levenscyclus van ICT-systemen. Daarbij zet het ministerie zich onverminderd in om het niveau van bewustwording onder medewerkers te verhogen. Door (verplichte) trainingen, *e-learning*s en informatieberichten via verschillende kanalen (bijvoorbeeld via het Rijksportaal) worden medewerkers geïnformeerd over hoe om te gaan met persoonsgegevens om de kans op een datalek te verkleinen. Ook wordt informatie verstrekt over wat een datalek inhoudt, en hoe een datalek moet worden gemeld met als doel om de meldingsbereidheid van de medewerkers te vergroten.

- 17 Is er een plan om de fysieke ruimte van het ministerie aan te passen zodat de privacy hier gewaarborgd blijft en gevoelige informatie voldoende beschermd is? 18

Antwoord:

In goed overleg met het ministerie van BZK wordt gezien hoe de fysieke ruimte verder kan worden aangepast.

- 18 Doet de bij het departement geconstateerde situatie "dat er in open ruimtes of ruimtes die zijn afgeschermd met glazen wanden wordt gewerkt met gevoelige informatie" zich ook voor op posten in het buitenland? Zo ja, welke posten betreft dat? 18

Antwoord:

Op de posten gelden dezelfde regels ten aanzien van informatiebeveiliging als op het departement. In het geval van posten in landen met verhoogde inteldreiging wordt daar extra streng op toegezien. De komende periode zal de situatie op de posten opnieuw worden beoordeeld. Als zou worden geconstateerd dat er tekortkomingen zijn, dan worden die op zo kort mogelijke termijn geadresseerd.

- 19 Welke wijzigingen zijn doorgevoerd nadat bleek dat de ICT-beveiliging niet op orde was? 18

Antwoord:

Het ministerie heeft het beleid binnen het genoemde ICT-systeem aangepast van ‘open tenzij’ naar ‘gesloten, tenzij’ waardoor oneigenlijke inzage niet meer mogelijk zal zijn.

- 20 Is er onderzocht of er in de thuiswerksituatie vertrouwelijke informatie voldoende beschermd wordt tegenover bijvoorbeeld huisgenoten? 19

Antwoord:

Het ministerie heeft hier geen eigen concreet onderzoek naar uitgevoerd. Er is gedurende het afgelopen jaar wel regelmatig aandacht gevraagd voor veilig thuiswerken. Zo zijn er berichten geplaatst op het Rijksportaal met tips voor veilig thuiswerken, waaronder het afschermen en tijdig afsluiten van de digitale werkomgeving. Informatie met een hoger vertrouwelijkheidsniveau, waaronder EU en NAVO informatie, dient op het departement of kanselarij te worden gelezen.

- 21 Hoeveel WhatsApp-accounts van werknemers zijn in 2020 overgenomen door criminelen? 19

Antwoord:

Het ministerie heeft in de afgelopen maanden tientallen meldingen ontvangen van medewerkers over pogingen tot WhatsApp fraude. Het precieze aantal medewerkers dat slachtoffer is geworden van deze fraude is niet bekend. Dit mede omdat medewerkers ook gebruik maken van eigen telefoons. De instructie voor het ongedaan maken is door de servicedesk en beveiligingsadviseurs met de getroffen werknemers gedeeld.

Het ministerie adviseert in algemene zin medewerkers terughoudend te zijn in het gebruik van messaging apps. Dergelijke apps zijn niet geschikt voor communicatie van gevoelige informatie. Ook wordt actief gewaarschuwd voor veel voorkomende hackvormen.

- 22 Is de nieuw vastgestelde bezettingsnorm voor het gebouw van het ministerie van Buitenlandse Zaken coronaproof? 23

Antwoord:

Nee hier is nog geen rekening gehouden met de 1,5 m. kantooromgeving.

- 23 Welke norm voor werkplekken/fte wordt er op andere ministeries gebruikt? Hoe is de tevredenheid op deze andere ministeries? 24

Antwoord:

Deze vraag dient te worden gesteld aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Vanuit de verantwoordelijkheid voor het ministerie van Buitenlandse Zaken kan ik geen uitspraak doen over normen en tevredenheid van andere ministeries.

- 24 Hoe wordt het aandeel thuiswerken na de coronacrisis voorzien? Is de opschaling naar 0.9 werkplek/fte dan nog steeds nodig, of is er nog meer nodig? 24

Antwoord:

Het is op dit moment moeilijk in te schatten hoeveel medewerkers na de Coronapandemie thuis of hybride zullen gaan werken. Daar komt bij dat voor de pandemie in het pand al sprake was van overbezetting. Vooralsnog wordt dan ook niet uitgegaan van een effect op de benodigde werkpleknorm. Wij zullen eerst ervaring op moeten doen met de nieuwe (post-COVID) situatie.

- 25 Wordt er naast het opschalen van het aantal werkplekken, ook gewerkt aan de andere problemen zoals de geluidsoverlast door te veel werkplekken in één ruimte? 24

Antwoord:

Ja er is een pilot geweest voor akoestiek en belcellen. De pilot is positief ontvangen en wordt verder uitgerold. In de discussie rondom hybride werken wordt op dit moment nagedacht over hoe grote open werkruimten ingericht kunnen worden als stilteruimte.

- 26 Wat is er sinds het instellen van de nieuwe norm gedaan om het gebouw te laten voldoen aan die norm? 24

Antwoord:

De normproblematiek zal in een aankomend masterplan Huisvesting Den Haag worden meegenomen. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties voert hierop de regie.

- 27 Kunt u bevestigen dat de toegangsbeveiliging niet voldoet aan de eisen van de NAVO? Is Nederland hierover door de NAVO op de vingers getikt? Binnen welke termijn kunnen de noodzakelijke aanpassingen worden doorgevoerd en hoe hoog schat u de kosten in? 26

Antwoord:

Het gebouw aan de Rijnstraat 8 kent verschillende zones met een oplopend beveiligingsniveau (van publiek naar gesloten). De zwaarder beveiligde zones zijn alleen toegankelijk voor geautoriseerde medewerkers. Het probleem is dat de toegang vanuit de publieke zone naar de meer beveiligde zones onvoldoende

is beveiligd waardoor niet geautoriseerde medewerkers en bezoekers makkelijk toegang kunnen krijgen tot de beveiligde zones. In het veelal uit open ruimtes bestaande werkgebied van het ministerie van BZ wordt gewerkt met gevoelige informatie; persoonsgegevens, departementaal vertrouwelijke informatie en de EU- en NAVO equivalenten hiervan. In de rapporten van de inspecties merken zowel EU als NAVO op dat er een risico van meelopen is. BZK voert op dit moment een onderzoek uit hoe dit risico verholpen kan worden.

- 28 Wat is er sinds het constateren van het probleem met fysieke veiligheid (meelopen) gedaan om dat probleem op te lossen? 26

Antwoord:

Tot op heden is er een aantal stappen gezet:

Er is een bewustwordingscampagne gestart waarin wordt gefocust op de gesignaleerde risico's. Het bestuursplein op de 7^e etage is uitsluitend toegankelijk gemaakt voor BZ'ers. Het zichtbaar dragen van de Rijkspas wordt verplicht gesteld. Er is inmiddels een projectleider benoemd vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties voor het ontwikkelen van een scenario voor de fysieke beveiliging.

- 29 Zijn er sinds 2018/2019 nog stappen gezet in het meer representatief ontvangen van buitenlandse gasten, aangezien er duidelijk nog problemen zijn? Zo ja, welke stappen zijn dit? Zo nee, waarom zijn deze stappen niet gezet? 27

Antwoord:

Bij ieder bezoek van buitenlandse hoogwaardigheidsbekleders wordt door Protocol gestreefd de representatie zo optimaal mogelijk uit te voeren. Hierbij is het afgelopen jaar uiteraard rekening gehouden met de beperkingen in verband met de corona-regels.

De mogelijkheden voor de medewerkers van de Rijksbeveiligingsorganisatie (RBO) om bij binnenkomst en vertrek Protocol bij te staan zijn in 2018/19 verruimd. Deze bijstand bestaat uit het openen van de zijdeur, zodat de 'VIP' niet door de draaideur hoeft (dat is nl. ongewenst en onveilig), het open houden van de sluis en het assistentie verlenen bij de twee liften. De 'VIP' kan dan met beveiliging, protocol en 1 delegatielid in de bewindslidenlift, terwijl andere delegatielieden gebruik kunnen maken van de tegenover gelegen goederenlift. Het is nl. altijd de bedoeling dat alle leden van een delegatie tegelijkertijd omhoog en omlaag gaan.

Qua representativiteit is er een aantal, binnen de fysieke mogelijkheden van het gebouw, cosmetische aanpassingen aangebracht. Het betreft het schilderen van de lifthallen en het herinrichten van de VIP ontvangstruimte. Met de gemeente wordt verder overlegd over de herinrichting van de buitenruimte aan de VIP zijde (bijv. de positionering van de vlaggenmasten).

- 30 Worden er in de toekomst stappen gezet om de nog bestaande problemen met betrekking tot het representatief ontvangen van buitenlandse gasten op te lossen? 27

Antwoord:

Het gebouw kent grote beperkingen. Mede om die reden wordt samen met het ministerie van BZK gezocht naar oplossing in het kader van het huisvestingsplan Den Haag.

- 31 Welke beveiligingsrisico's zijn er voor buitenlandse gasten door gebreken aan het gebouw? 27

Antwoord:

Wegens het ontbreken van een volwaardige separate ingang voor hoogwaardigheidsbekleders, zoals in gebouw aan de Bezuidenhoutseweg 67 "B67" wel het geval was, betreden deze het gebouw doorgaans aan de zijde van de Schedeldoekshaven. Vanuit beveiligingsoogpunt is dit onwenselijk, aangezien dat een openbare ruimte betreft waar vaak veel publiek aanwezig is.

- 32 Zorgen de gebreken aan het gebouw met betrekking tot het ontvangen van buitenlandse gasten ervoor dat het ministerie minder goed haar werk kan doen? 27

Antwoord:

Zeker in vergelijking met het gebouw aan de Bezuidenhoutseweg 67 zijn de faciliteiten beperkt en is onvoldoende representatief en in het diplomatieke verkeer, zeker bij hoogwaardigheidsbekleders, is een zeker decorum usance. Ook de beveiliging van belangrijke gasten is een aspect (zie vraag 31). Binnen de genoemde beperkingen zorgt het ministerie zo goed als mogelijk voor protocollaire begeleiding.

- 33 Kunt u aangeven waarom het bestaande evacuatieplan niet is gebruikt tijdens de repatriëring aan het begin van de corona-crisis? 33

Antwoord:

De Algemene Rekenkamer constateert dat het bestaande evacuatiebeleid in grote lijnen is gevolgd. Dit mede dankzij de inzet van ervaren consulaire medewerkers in een speciaal hiervoor opgericht crisisteam. Dat beleid geeft de kaders weer voor evacuatie (onder andere opties voor de wijze waarop transport kan worden georganiseerd, in samenwerking met andere EU-landen of bijvoorbeeld met private partners). Er bestaat geen centraal en gedetailleerd evacuatieplan, omdat dat geen recht zou doen aan de heel verschillende situaties die zich kunnen voordoen. Sommige ambassades hebben gezien de veiligheidssituatie wel evacuatieplannen maar die waren niet berekend op deze pandemie. De snelle ontwikkelingen en de omvang van de crisis zorgden ervoor dat een unieke en grootschalige publiek private samenwerking tot stand is gekomen. De belangrijkste lessen hieruit voor een crisis van een dergelijke omvang (onder andere qua registratie, en organisatiestructuur) zullen meegenomen om de crisisprotocollen te verrijken. Het trainen van medewerkers is hier onderdeel van.

- 34 Was het bestaande evacuatieplan, met de kennis van vandaag, adequaat? 33

Antwoord:

Het bestaande evacuatiebeleid geeft de geldende kaders weer voor evacuatie. Er bestaat geen centraal en gedetailleerd evacuatieplan, omdat dat geen recht zou doen aan de heel verschillende situaties die zich kunnen voordoen. Sommige ambassades hebben gezien de veiligheidssituatie wel evacuatieplannen maar die waren niet berekend op deze pandemie. De situatie die vanaf maart 2020 ontstond door de COVID-19-pandemie was zonder enig precedent. Tot dan toe bestonden ervaringen met evacuaties uit operaties gericht op één land of enkele locaties in één regio. Dat stelde het ministerie voor nieuwe uitdagingen onder andere qua registratie, organisatiestructuur, en financiering. Mede daarom is ook het BBB-convenant met externe private partijen tot stand gekomen.

- 35 Is het ministerie voornemens een nieuw evacuatieplan op te stellen? 33

Antwoord:

Op basis van de inzichten die zijn opgedaan door het Verantwoordingsonderzoek van de Algemene Rekenkamer, een interne evaluatie en een externe evaluatie door COT, Instituut voor Veiligheids- en Crisismanagement, zullen de crisisprotocollen en waar nodig zullen ook de kaders voor evacuatie aangepast worden t.b.v. inzet in een toekomstige crisis van een dergelijke omvang.

- 36 Op welke wijze gebruikt – of overweegt – het ministerie van Buitenlandse Zaken het toepassen van blockchain-technologie bij bijvoorbeeld het bijhouden van reizigersgegevens of het bewaren en delen van vertrouwelijke informatie? Heeft het ministerie specialisten op dit gebied in dienst of maakt het van de expertise van anderen gebruik? 33

Antwoord:

Binnen het Ministerie van Buitenlandse Zaken (BZ) wordt geen gebruik gemaakt van Blockchain technologie. Op het moment van schrijven wordt ook niet voorzien een dergelijke technologie toe te passen. Dit omdat andere technologieën beter aansluiten op de behoeften en doelen van het ministerie. BZ volgt de opkomst van deze nieuwe technologieën wel en onderzoekt of er mogelijke toepassingen zijn. Het ministerie heeft op dit moment geen eigenblockchainspecialisten in dienst.

- 37 Zijn er mensen die geëvacueerd zijn onder de Bijzondere Bijstand Buitenland (BBB) die aangeven financiële moeite te hebben met het terugbetalen? Zo ja, hoeveel? 35

Antwoord:

In totaal hebben 1.633 reizigers gebruik gemaakt van een betaalregeling, hiervan hebben 360 reizigers de eigen bijdrage (nog) niet volledig voldaan. Aan 20 reizigers is de eigen bijdrage kwijtgescholden vanwege het feit dat zij deze niet

kunnen betalen. In de afhandeling van de betaalregeling wordt zorgvuldig maatwerk toegepast.