Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

DG Digitalisering & Overheidsorganisatie
DGDOO-CIO Rijk/IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag

Datum 25 juni 2026
Betreft Beantwoording Kamervragen van het lid Van den Berg (JA21) over digitale soevereiniteit, kritieke digitale overheidsinfrastructuur en de afhankelijkheden rond DigiD, Solvinity en Kyndryl.

Onze referentie
2026-0000294466

Hierbij zend ik u, mede namens de staatssecretaris Digitale Economie en Soevereiniteit, de antwoorden op de vragen van het lid Van den Berg (JA21) over digitale soevereiniteit, kritieke digitale overheidsinfrastructuur en de afhankelijkheden rond DigiD, Solvinity en Kyndryl. Ingezonden 4 juni 2026, 2026Z12034.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Eric van der Burg

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

Vragen van het lid Van den Berg (JA21) *(2026Z12034)* aan de staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken en Klimaat en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie en Veiligheid over digitale soevereiniteit, kritieke digitale overheidsinfrastructuur en de afhankelijkheden rond DigiD, Solvinity en Kyndryl. Ingezonden 4 juni 2026.

1. Kunt u toelichten waarom de voor DigiD benodigde digitale infrastructuur en diensten niet rijksbreed zijn georganiseerd, maar via afzonderlijke aanbestedingen en contracten worden ingekocht? Welke afwegingen liggen hieraan ten grondslag?

De genoemde voorzieningen zijn rijksbreed georganiseerd. Logius is rijksbreed verantwoordelijk voor het beheer en de doorontwikkeling van voorzieningen als DigiD. De verschillende leveranciers die hierbij zijn betrokken zijn geselecteerd via verschillende Europese aanbestedingen. Logius maakt hierbij gebruik van geldende regels rondom aanbestedingen en van rijksbrede kaders ten aanzien van digitalisering, zoals bijvoorbeeld het Rijkscloudbeleid.
Bij het vormgeven van deze aanbestedingen stond de ondersteuning van de continuïteit van de dienstverlening, digitale weerbaarheid en efficiënt gebruik van IT-diensten centraal.

De voorkeur is om op langere termijn gebruik te maken van de soevereine overheidscloud voor de levering van het platform, infrastructuur en datacenters. Hiervoor is het van essentieel belang dat de overheidscloud klaar is om de continuïteit en veiligheid van Logius dienstverlening te waarborgen.

2. Wanneer gaat het kabinet kritieke digitale overheidsvoorzieningen, zoals DigiD, MijnOverheid, Digipoort en vergelijkbare voorzieningen, wél rijksbreed organiseren of ten minste rijksbreed normeren?

De genoemde voorzieningen zijn rijksbreed georganiseerd. Logius voert het beheer uit van deze overheidsvoorzieningen ten behoeve van andere overheidsdienstverleners. De normering voor risicomanagement en cybersecurity volgt uit de Cyberbeveiligingswet (Cbw).

3. Hoe en wanneer geeft het kabinet uitvoering aan de aangenomen motie-Van den Berg c.s. over een rijksbreed dataclassificatie- en datalocatiebeleid (Kamerstuk 26 643, nr. 1482)?

De motie verzoekt het opstellen en uitrollen van een rijksbreed dataclassificatie- en datalocatiebeleid. Een rijksbreed dataclassificatiebeleid is reeds vastgesteld in het VIR-BI 2025. Daarbij geldt dat voor de zwaarste categorieën (Staatsgeheim, of Te Beschermen Belangen 1-3) het gebruik van publieke cloud niet toegestaan is. Wanneer voor de opslag en verwerking van dergelijk gerubriceerde data een externe leverancier wordt overwogen, moet deze leverancier voldoen aan de eisen van de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO). De ABRO stelt onder andere eisen aan sleutelbeheer voor encryptie. Controle of de leverancier hieraan voldoet, bij zowel aanvang als tijdens de looptijd van de overeenkomst wordt gecontroleerd door het Nationaal Bureau Industrie Veiligheid (NBIV). De ABRO is in december 2025

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

goedgekeurd, organisaties krijgen twee jaar de tijd om de ABRO in te voeren, daarom verschilt de ingangsdatum per organisatie. Andere overheidsonderdelen en leveranciers die onder de Wet weerbaarheid kritieke entiteiten vallen, kunnen in de toekomst verplicht worden de ABRO te gebruiken.

Daarnaast stelt het huidige rijksbreed cloudbeleid dat de data bij gebruik van publieke clouddiensten moet worden verwerkt binnen de landen van de Europese Economische Ruimte (EER), in landen waarvoor de Europese Commissie een adequaatheidsbesluit heeft genomen, of in landen die anderszins voldoen aan de eisen van art. 46, AVG. De uit te voeren risicoanalyse, onderdeel van het beleid, geeft de organisatie ook inzichten in de vraag of het land van de cloudprovider via extraterritoriale wetgeving toegang kan krijgen tot de data. Daarnaast moeten er plannen ter schadebeperking worden overwogen. Dit is een vorm van het door u voorgestelde te implementeren localisatiebeleid.

Later dit jaar wordt het herziene rijksbrede cloudbeleid met uw Kamer gedeeld. De werking van het cloudbeleid wordt verbreed van de rijksdienst naar de rijksoverheid. Ook is er in dit beleid meer aandacht voor geopolitieke risico's in situaties waarin een leverancier (mede) onder een niet-Europese jurisdictie valt. Voor bepaalde toepassingen wordt het gebruik van dergelijke leveranciers of van de publieke cloud niet langer toegestaan. Op deze manier zijn wij voornemens om de motie uit te voeren.

4. Welke concrete stappen zijn sinds aanneming van deze motie gezet, welke bewindspersoon is eerstverantwoordelijk en wanneer ontvangt de Kamer een voortgangsrapportage?

Zoals toegelicht in het antwoord op vraag 3 ontvangt de Kamer dit jaar het herziene rijksbrede cloudbeleid 2026. Daarnaast stelt de Rijksoverheid voor gevoelige overheidsdata en processen beveiligingseisen verplicht op basis van de BIO2 via de Cyberbeveiligingswet (Cbw). Verder wordt het belang van "veilig inkopen" en de risico's van mogelijke buitenlandse inmenging in toenemende mate erkend. De ABRO stelt eisen aan de veiligheid bij de leverancier. Waar uit de risicoanalyses blijkt dat het risico van statelijke actoren reëel is, bieden de BIO2, de Aanbestedingswet op defensie- en veiligheidsgebied (ADV) en ABRO (de laatste twee in het kader van inkoop), middelen om de risico's goed te beheren. Op basis van deze beleidskaders en wettelijke verplichtingen worden overheidsorganisaties geholpen bij het maximaal beschermen van data en beveiligingsmaatregelen. Aan de hand van deze kaders, zoals het uitvoeren van een risicoanalyse, kunnen organisaties zelf vaststellen hoe en waar zij data veilig kunnen opslaan en bewerken.

Daarnaast wordt op dit moment, in het kader van de Nederlandse Digitaliseringsstrategie, gewerkt aan de verkenning naar de realisatie van een soevereine overheidscloud. Dit zal hand in hand gaan met de verdere ontwikkeling van het daarmee samenhangende beleid.

De Rijksoverheid versterkt continu haar integrale weerbaarheid. Binnen dit verband, zoals toegelicht in deze brief, zijn de afgelopen jaren verschillende beveiligingskaders, -normen en wetten aangepast zoals VIR-BI2025, BIO2, de ABRO. Ook bereiden we ons

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

voor op aankomende wetgeving zoals de Wet weerbaarheid kritieke entiteiten (Wwke) en de Cbw. De effectieve toepassing van deze wetten verhoogt de basisbeveiliging, zoals ook het beheer en opslag van data van overheidsorganisaties. Gezien het feit dat een deel van deze regelgeving pas recent is ingegaan of op korte termijn ingaat, en gelet op de nadere verwachte EU wet- en regelgeving op dit gebied, kies ik er vooralsnog voor nu geen aanvullend beleid te maken, maar eerst te bezien of de nieuwe wet- en regelgeving ook de beoogde verbetering van weerbaarheid bereikt.

5. Welke voorzieningen kwalificeert het kabinet, naast DigiD, als kritieke digitale overheidsinfrastructuur?

Op dit moment ligt dat besloten in de “Aanpak Vitaal”. Deze wordt later dit jaar vervangen door de Wet weerbaarheid Kritieke Entiteiten (Wwke). De betrokken vakministers bepalen welke overheidsvoorzieningen onder deze wet zullen vallen.

6. Bestaat er inmiddels een rijksbreed overzicht van kritieke digitale overheidsvoorzieningen en de daarbij betrokken niet-Nederlandse of niet-Europese leveranciers? Zo nee, waarom niet?

Er bestaat geen rijksbreed overzicht van kritieke digitale overheidsvoorzieningen.
Het Besluit beveiliging netwerk- en informatiesystemen (Bbni) stelt eisen aan aanbieders ten aanzien van de beveiliging van ICT-systemen. De later dit jaar van kracht wordende Cyberbeveiligingswet stelt eisen aan risico- en ketenmanagement. Daarmee zullen overheidsorganisaties die kritieke digitale overheidsvoorzieningen beheren, inzage moeten hebben in welke niet-Nederlandse of niet-Europese leveranciers in de keten een rol spelen. De mogelijke risico’s daarvan moeten worden beoordeeld en worden gemitigeerd of geaccepteerd.
Er bestaat geen centraal register van dergelijke leveranciers per kritieke overheidsvoorziening. Als reactie op het onderzoek ‘Van Kwetsbaar naar weerbaar’, dat is uitgevoerd in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, wordt door de Taskforce Continuïteit ICT Dienstverlening een pilot uitgevoerd voor het monitoren van belangrijke leveranciers voor de overheid.

7. Wanneer komt er een dergelijk overzicht, inclusief inzicht in cloud, hosting, beheer, datatoegang, encryptiesleutels, operationele zeggenschap, onderaannemers, ketenafhankelijkheden en exittermijnen?

Een dergelijk overzicht is er niet. Het is in het kader van veiligheid ook niet wenselijk dat er een dergelijk overzicht komt. Dergelijke data op één plaats vastleggen zou namelijk een operationeel veiligheidsrisico vormen.

8. Wat is het doel van het kabinet ten aanzien van de toekomstige inrichting van DigiD? Is het streven gericht op andere technologie, een andere leverancier, Europese of Nederlandse zeggenschap, publiek beheer of een combinatie daarvan?

Het streven is met name gericht op het vormgeven van het nieuwe aanbestedingstraject op basis van de aanbestedingswet Defensie en Veiligheid (ADV), zoals vermeld in de

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

Kamerbrief van 4 juni jl.[1] Deze aanbesteding ziet op het opnieuw aanbesteden van het beheer van het huidige platform. De ADV biedt meer mogelijkheden dan een reguliere Europese aanbesteding om risico's voor de nationale veiligheid te beperken. Zodra een nieuwe leverancier is geworven, zal er een overdracht moeten plaatsvinden. Omdat het maatwerk betreft, is kennis van en ervaring met het platform noodzakelijk om de Logius-voorzieningen goed te laten draaien. Hiervoor wordt een periode van 6-12 maanden gehanteerd.

De voorkeur is om op langere termijn gebruik te maken van de soevereine overheidscloud voor de levering van het platform, infrastructuur en datacenters.

9. Welke rol speelt digitale soevereiniteit precies bij de toekomstige inrichting van DigiD? Welke concrete risico's worden hiermee beoogd te verminderen?

Zoals hiervoor aangegeven biedt een ADV-aanbesteding meer mogelijkheden dan een reguliere Europese Aanbesteding om risico's voor de nationale veiligheid te beperken. Op dit moment treft Logius de voorbereidingen voor het uitvoeren van de aanbesteding.

10. Hoe verhoudt het Nederlandse beleid zich tot landen die eveneens streven naar digitale autonomie, maar daarbij gebruikmaken van technologie van niet-Europese aanbieders?

Er is geen overzicht van keuzes die andere Europese landen maken voor het inrichten van hun digitale infrastructuur. In de 'Verkenning naar de soevereine overheidscloud' in het kader van de NDS wordt een eerste set keuzes voor de vormgeving van een soevereine overheidscloud gepubliceerd. Deze wordt naar verwachting vóór het zomerreces nog aan uw Kamer verstuurd.

De Europese Commissie heeft recent het voorstel voor de Cloud and AI Development Act (CADA) gepubliceerd. Deze verwoordt de ambitie van de Commissie om te komen tot sterkere en uniforme eisen aan de soevereiniteit van door overheden gebruikte cloudoplossingen. Het Nederlandse beleid zal in de toekomst hier verder op afgestemd worden. De verwachting is dat overheden in lidstaten als gevolg van de CADA op een uniforme manier risicobeoordelingen maken voor het gebruik van public clouddiensten en gebruik zullen maken van passende, erkende soevereine clouddiensten. Een BNC-fiche over het wetsvoorstel voor de CADA wordt op korte termijn met de Tweede Kamer gedeeld.

11. In de kabinetsreactie van 23 mei 2025 op de motie-Koekkoek (Kamerstuk 26643, nr. 1338) werd gesteld dat er kwalitatief hoogwaardige Europese clouddiensten beschikbaar zijn. Op welke concrete marktverkenning, technische toets of aanbestedingservaring was die conclusie gebaseerd? Zag die conclusie bovendien op generieke clouddiensten, of ook op kritieke digitale identiteitsinfrastructuur zoals DigiD, MijnOverheid en Digipoort?

In de genoemde Kamerbrief[2] wordt gesteld dat deze conclusie gebaseerd is op een

[1] Kamerbrief over stand van zaken aanvullende maatregelen Logius in relatie tot Solvinity | Open.overheid.nl
[2] Kamerbrief over Europese cloud-alternatieven | Rijksoverheid.nl

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

quickscan onderzoek naar de verschillen in technische, juridische en organisatorische aspecten van het dienstenaanbod van Nederlandse en Europese aanbieders van clouddiensten ten opzichte van de drie grootste aanbieders van buiten de EU. Dit onderzoek is in opdracht van het ministerie van Economische Zaken en Klimaat uitgevoerd door KPMG.[3] Dit onderzoek zag op de gehele markt voor clouddiensten en had geen specifieke focus op kritieke digitale identiteitsinfrastructuur.

12. Welke concrete stappen zijn tussen 23 mei 2025 en 2 juni 2026 gezet om Nederlandse of Europese alternatieven daadwerkelijk geschikt te maken voor het beheer van DigiD of vergelijkbare kritieke voorzieningen?

De ADV-aanbesteding biedt meer mogelijkheden dan een reguliere Europese aanbesteding om risico's voor nationale veiligheid te beperken. In de aanbestedingsfase worden de (beveiligings)technische en operationele eisen gesteld waaraan een leverancier moet voldoen om in aanmerking te komen. Deze eisen zijn specifiek toegesneden op het beheer van kritieke digitale infrastructuur op nationale schaal. Op dit moment treft Logius de voorbereidingen voor het uitvoeren van de aanbesteding onder de ADV.

13. In eerdere beantwoording heeft u gesteld dat sprake is van gelijkwaardige technologieën van Europese en Nederlandse aanbieders. Wat verstaat het kabinet precies onder een "gelijkwaardig alternatief" voor de huidige DigiD-dienstverlening?

Onder een gelijkwaardig alternatief verstaat het kabinet andere Nederlandse en Europese IT-dienstverleners die in staat zijn om diensten te leveren die functioneel, kwalitatief en beveiligingstechnisch vergelijkbaar zijn met de dienstverlening die Solvinity momenteel aan Logius levert, namelijk de beheerwerkzaamheden van het PICARD-platform. Het gaat daarbij om aanbieders die aantoonbaar kunnen voldoen aan de eisen voor continuïteit, beveiliging, compliance en schaalbaarheid van de DigiD-dienstverlening.

14. Welke criteria worden gehanteerd om vast te stellen of een alternatief gelijkwaardig is? Wordt daarbij gekeken naar functionaliteit, schaalbaarheid, beveiliging, beschikbaarheid, betrouwbaarheid, certificeringen, prestaties, migratierisico's, operationele ervaring, continuïteit en bewezen beheer van kritieke digitale infrastructuur op nationale schaal?

Criteria worden verwoord en van weging voorzien gedurende het proces om te gaan aanbesteden, bij het uitvragen van een behoefte naar de algehele markt en conform processen die voortvloeien uit diverse kaders (financieel, juridisch, technisch, etc.). Een opdrachtgever is hiervoor verantwoordelijk en zal daarbij ondersteund worden door een multidisciplinair team. Het wisselt dus per opdrachtgever en per opdracht welke criteria gehanteerd worden (dan wel hoe zwaar die wegen). De hele gedachte van een aanbestedingsproces is om de pluraliteit van de markt te benutten en een te grote afhankelijkheid te vermijden.

[3] KPMG (2024) – Eindrapport in het kader van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers.

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

15. Deelt u de opvatting dat DigiD vanwege zijn unieke en kritieke rol moeilijk één-op-één vergelijkbaar is met generieke cloud-, hosting- of authenticatiediensten? Zo nee, waarom niet? Zo ja, kunt u toelichten hoe deze unieke rol van DigiD zich verhoudt tot de conclusie van de ACM dat er voldoende concurrentie overblijft omdat er andere IT-dienstverleners zijn die soortgelijke diensten leveren?

Zoals in het antwoord op vraag 8 aangegeven betreft de technische inrichting van DigiD maatwerk. Omdat het maatwerk betreft, is kennis van en ervaring met het platform noodzakelijk om de Logius-voorzieningen goed te laten draaien. In de overdrachtsperiode van 6-12 maanden kan een nieuwe contractant deze ervaring opbouwen.

16. Wat verstaat het kabinet in dit verband onder "soortgelijke diensten"? Gaat het daarbij om algemene IT-dienstverlening, of specifiek om bewezen beheer van kritieke digitale identiteitsinfrastructuur op nationale schaal?

In het geval van DigiD en andere Logius-voorzieningen verstaat het kabinet onder "soortgelijke" diensten het overnemen van de beheerwerkzaamheden van het PICARD-platform. In de aanbestedingsfase worden de (beveiligings)technische en operationele eisen gesteld waaraan een leverancier moet voldoen om in aanmerking te komen. Deze eisen zijn specifiek toegesneden op het beheer van kritieke digitale infrastructuur op nationale schaal.

17. Welke minimale eisen gelden voor cloud, hosting, beheer, encryptiesleutels, toegangsbeheer, logging, monitoring, incidentrespons, onderaannemers en operationele zeggenschap bij DigiD?

DigiD voldoet aan strenge eisen en regelgeving rondom veiligheid en privacy. Daarvoor worden verschillende vormen van toegangsbeveiliging en versleuteling toegepast.

Alle informatie over de werking van DigiD is terug te vinden op de website van Logius. Op de website is alle documentatie terug te vinden ten aanzien van het aansluiten op DigiD door afnemers, de functionele beschrijvingen van DigiD (inclusief verwerking persoonsgegevens), en de technische documentatie over de werking van DigiD.

U kunt de informatie terugvinden via de volgende link: https://www.logius.nl/onze-dienstverlening/toegang/digid/documentatie

18. Hoe wordt geborgd dat encryptiesleutels, beheerrechten en operationele toegang tot DigiD niet onder zeggenschap vallen van niet-Europese moederbedrijven of buitenlandse wettelijke bevoegdheden?

Op 21 mei jl. bent u middels een vertrouwelijke technische briefing geïnformeerd over de situatie bij Logius. Daarnaast biedt een aanbesteding via de ADV mogelijkheden om risico's voor de nationale veiligheid te beperken.

DG Digitalisering & Overheidsorganisatie
DGDOO-IFHR-Inkoop- & Aanbestedingsbeleid
Taskforce Continuïteit ICT Dienstverlening

Onze referentie
2026-0000294466

19. Heeft iedere kritieke digitale overheidsvoorziening een actueel exitplan? Zo ja, hoe vaak worden deze exitplannen getest?

Het, nog vast te stellen, herziene rijksbrede cloudbeleid scherpt de eis van een exitstrategie aan naar het hebben van een exitplan. Dat exitplan moet jaarlijks op actualiteit worden beoordeeld. Exitplannen zijn contractuele afspraken over de (geplande of plotselinge) afronding van een contract. Het is wel van belang dat hierin realistische afspraken worden opgenomen afhankelijk van de situatie en context van de specifieke voorziening.
De aanstaande Wet weerbaarheid kritieke entiteiten stelt eisen aan de weerbaarheid en continuïteit van de dienstverlening voor organisaties die daaronder vallen. Dit geldt eveneens als er geen gebruik van clouddiensten wordt gemaakt.

20. Welke kritieke digitale voorzieningen hebben een verwachte migratietermijn van meer dan zes maanden, en welke continuïteitsrisico's levert dat op?

Zie het antwoord op vraag 6. Daarnaast is – gezien de aanbestedingsverplichtingen waar overheidsorganisaties aan dienen te voldoen – zes maanden überhaupt een zeer korte termijn. Het herziene rijksbrede cloudbeleid geeft aan dat de rijksoverheid organisaties beschikken over een exitplan waarin ook rekening wordt gehouden met het onverwacht niet-beschikbaar zijn van de gebruikte clouddienst. De organisatie moet een plan maken hoe de betrokken overheidsdienst binnen acceptabele termijn kan worden hersteld. De meeste migraties nemen meer tijd in beslag. Migratietermijnen kunnen vanuit technisch oogpunt jaren duren, afhankelijk van de type dienstverlening en kenmerken.

21. Welke onderdelen van de TFEV- of BTI-analyse rond Solvinity/Kyndryl kunnen openbaar met de Kamer worden gedeeld, en welke onderdelen kunnen vertrouwelijk worden verstrekt?

Wat betreft de analyse van het Bureau Toetsing Investeringen (BTI) maakt het kabinet de onderliggende adviezen, risicoanalyses en vertrouwelijke overwegingen die ten grondslag liggen aan een advies niet openbaar. Deze stukken bevatten vertrouwelijke bedrijfsinformatie en informatie die raakt aan de bescherming van de nationale veiligheid. Openbaarmaking zou afbreuk kunnen doen aan de belangen die de wet juist beoogt te beschermen. Wat betreft de bespreking in de Taskforce Economische Veiligheid (TFEV) geldt dat ook deze vertrouwelijk is en informatie bevat die raakt aan de bescherming van de nationale veiligheid. Het kabinet hecht tegelijkertijd aan een goede informatievoorziening van de Kamer. Daarom is de Kamer in de gelegenheid gesteld om in de vertrouwelijke technische briefing van 10 juni jl. te worden geïnformeerd over de analyse en toetsing onder de Wet ongewenste zeggenschap Telecommunicatie die door BTI is verricht en met advies aan de staatssecretaris Digitale Economie en Soevereiniteit is voorgelegd.

22. Kunt u de vragen afzonderlijk en voor het commissiedebat inzake Bescherming persoonsgegevens en grote datalekken van 25 juni aanstaande beantwoorden?

Ja