36 945 VI Jaarverslag en slotwet Ministerie van Justitie en Veiligheid 2025

36 945 VII Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2025

36 945 XIII Jaarverslag en slotwet Ministerie van Economische Zaken 2025

Nr. 11 LIJST VAN VRAGEN EN ANTWOORDEN
Vastgesteld 9 juni 2026

De vaste commissie voor Digitale Zaken heeft een aantal vragen voorgelegd aan de ministers van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties en Koninkrijkrelaties, en van Economische Zaken en Klimaat inzake het rapport Resultaten verantwoordingsonderzoek 2025 bij het Ministerie van Justitie en Veiligheid (Kamerstuk 36945-VI-2); het rapport Resultaten verantwoordingsonderzoek 2025 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 36945-VII-2); het rapport Resultaten verantwoordingsonderzoek 2025 bij het Ministerie van Economische Zaken (Kamerstuk 36945-XIII-2).

De vragen en opmerkingen zijn op 27 mei 2026 aan de ministers van Justitie en Veiligheid, van Binnenlandse Zaken en Koninkrijksrelaties en Koninkrijkrelaties, en van Economische Zaken en Klimaat voorgelegd. Bij brief van 9 juni 2026 zijn de vragen beantwoord.

De voorzitter van de commissie,
Dekker

Adjunct-griffier van de commissie,
Muller

Vragen en antwoorden inzake Resultaten verantwoordingsonderzoek 2025 bij het Ministerie van Justitie en Veiligheid (36945-VI-2)

Vraag 1

Hoe verklaart u de trends rondom online criminaliteit?

Antwoord

De trends zoals opgenomen in het verslag van de Algemene Rekenkamer komen uit de CBS Veiligheidsmonitor die aan de Kamer is aangeboden op 2 maart 2026. In 2025 hebben ruim 200.000 personen van 15 jaar en ouder de vragenlijst ingevuld.

- Politie en OM constateren dat de drempel voor online criminaliteit is verlaagd. Waar voorheen technische expertise vereist was, kunnen tegenwoordig kant-en-klare tools en handleidingen eenvoudig online worden aangeschaft via berichtendiensten en/of platforms (zoals Telegram, fora en het dark web). Ook het gebruik van AI speelt hierbij in toenemende mate een rol. Dit stelt individuen in staat om met minimale investering en technische kennis cyberaanvallen uit te voeren. Criminelen kunnen daarnaast met één handeling vaak vele mogelijke slachtoffers maken.
- De Kamer wordt over trends en ontwikkelingen in online criminaliteit geïnformeerd via de jaarlijkse Kamerbrieven over de voortgang van de integrale aanpak van cybercrime en de integrale aanpak online fraude.

De laatste Voortgangsbrief over de aanpak van cybercrime was op 25 juni 2025. De eerstvolgende voortgangsbrief cyber is voorzien in september 2026. Dan wordt ook de publicatie van een nieuw Cybercrimebeeld van OM en politie 2026 verwacht. In de Kamerbrief van 9 december 2025 is geïnformeerd over de stand van zaken en doorontwikkeling van de integrale aanpak online fraude. De volgende update over de aanpak online fraude wordt voor het zomerreces aan de Kamer aangeboden.

Vraag 2

Waarom heeft u nog geen opvolging gegeven aan de vorig jaar geconstateerde ICT-gerelateerde onvolkomenheden? Kunt u op alle drie de onvolkomenheden concreet ingaan?

Antwoord

Zoals geconstateerd door zowel de Audit Dienst Rijk (ADR) als de Algemene Rekenkamer (ARK) is er in 2025 opvolging gegeven én voortgang geboekt op de bevindingen (ADR) en onvolkomenheden (ARK) omtrent informatiebeveiliging. Hieronder kort uiteengezet de voortgang op de geconstateerde onvolkomenheden.

1. Accreditaties
Het afgelopen jaar is veel aandacht besteed aan het vergroten van de personele capaciteit voor accreditaties. Daarnaast heeft het interdepartementale accreditatiebeleid geleid tot het opstellen van een specifiek accreditatiebeleid JenV, het inrichten van een stelsel van accreditatieprocesbeschrijvingen en het opzetten van een kwaliteitsraamwerk. Op basis hiervan is gestart met het risico-gestuurd accrediteren van een aantal hoog-gerubriceerde informatiesystemen, waarmee wordt bijgedragen aan verbeterde bescherming van deze systemen tegen mogelijke beveiligingsincidenten zoals cyberaanvallen en datalekken. Een deel van de achterstand in de accreditatieverlening is hiermee weggewerkt.

2. Opvolging verbeterpunten uit beveiligingstesten
Het realiseren van deze verbeterpunten heeft een meerjarig karakter en kan daarmee niet binnen één jaar worden weggewerkt. Het hiervoor opgestelde verbeterplan voorziet onder meer in het bestendigen van redteamonderzoeken in de lijnorganisatie. Daarnaast wordt door middel van een periodieke kwaliteitscyclus voor redteamonderzoeken getoetst of de mitigerende maatregelen zijn geïmplementeerd en het gewenste beveiligingseffect wordt gerealiseerd.

3. Informatiedeling
Aan de informatie-uitwisseling tussen departement en JenV-organisaties over informatiebeveiliging wordt gewerkt, onder meer door het proces informatiedeling verder aan te scherpen en het toezicht daarop nader uit te werken. Verder is informatiebeveiliging vaker en met meer diepgang

onderwerp van bestuurlijk gesprek tussen departement en taakorganisaties.

Vraag 3

Hoe groot is de achterstand in de accreditatieverlening?

Antwoord

Accreditaties worden risico-gebaseerd opgepakt. Aan kritieke, hooggerubriceerde systemen en informatiesystemen die gerubriceerde informatie van EU of NAVO verwerken wordt voorrang gegeven. Van de informatiesystemen die aan voornoemde criteria voldoen zijn momenteel acht informatiesystemen geaccrediteerd en negen accreditatieonderzoek zijn lopen op het moment.

Vraag 4

Laat de achterstand in de accreditatieverlening zich alleen uitleggen door een gebrek aan personeel? Welke factoren spelen mogelijk nog een rol?

Antwoord

Het opbouwen van accreditatiedossiers met actuele en vastgestelde documentatie is een tijds- en arbeidsintensief proces voor de organisatieonderdelen, waardoor regelmatig wachttijden ontstaan. Dit wordt zo veel mogelijk ondervangen door gelijktijdig meerdere accreditatieonderzoeken op te starten, maar heeft desondanks, naast capaciteitsgebrek, een grote invloed op de snelheid waarmee achterstanden in de accreditatieverlening worden weggewerkt.

Een gestructureerde werkwijze (de Security Accreditatie Strategie) draagt bij aan een heldere werkwijze van het te doorlopen proces en de verwachte inspanning van de auditee.

Benadrukt wordt dat ondanks de druk om achterstanden weg te werken geen concessies worden gedaan aan kwaliteitsnormen.

Vraag 5

Welke opvolging geeft u aan beveiligingstesten van ethische hackers? Kunt u concreet uitleggen wat u met de uitkomsten doet of heeft gedaan, specifiek bij de drie door de Algemene Rekenkamer genoemde tekortkomingen?

Antwoord

Het realiseren van deze verbeterpunten heeft een meerjarig karakter en kan daarmee niet binnen één jaar worden weggewerkt. Het hiervoor opgestelde verbeterplan voorziet onder meer in het bestendigen van redteamonderzoeken in de lijnorganisatie. Daarnaast wordt door middel van een periodieke kwaliteitscyclus voor redteamonderzoeken getoetst of de mitigerende maatregelen zijn geïmplementeerd en het gewenste beveiligingseffect wordt gerealiseerd (d.m.v. herhaaltesten). Concreet zijn verder de volgende maatregelen getroffen in het kader van de genoemde tekortkomingen:

- Voor (netwerk)monitoring wordt gericht detectie software ingezet op (actuele) kwetsbaarheden.
- Ten aanzien van onveilig toegangsbeheer is departementaal beleid voor logging vastgesteld en worden tools ingezet voor verscherpt beheer en toezicht op het gebruik van gebruikersaccounts met hoge toegangsrechten.
- In het kader van het verbeteren van onveilig netwerkontwerp wordt beleid ontwikkeld voor netwerksegmentering.

Vraag 6

Welke voordelen heeft het decentraal beleggen van de informatiebeveiliging bij 70 JenV-organisaties? Welke risico’s kent dit stelsel?

Antwoord

Het decentraal beleggen van de verantwoordelijkheid voor informatiebeveiliging is in lijn met de aanstaande cyberbeveiligingswet (cbw). Het legt daarmee de verantwoordelijkheid in de bestuurskamer van de individuele organisatie en geeft hiermee aan dat informatiebeveiliging niet enkel een ICT probleem is. De taakorganisatie heeft

immers als geen ander kennis van de eigen (wettelijke en overige) kerntaken en mogelijke beveiligingsrisico's. Zicht houden op de staat van informatiebeveiliging is een inherent risico bij een decentraal stelsel.

Vraag 7

Hoe ziet u er op toe dat alle 70 JenV-organisaties een gelijke mate van cyberveiligheid kennen?

Antwoord

Voor de staat van de informatiebeveiliging bij taakorganisaties is het van belang dat risico's inzichtelijk zijn en erop wordt gestuurd. De informatie-uitwisseling die hiervoor nodig is wordt verbeterd, onder meer door het proces informatiedeling verder aan te scherpen en het toezicht daarop nader uit te werken. Verder is informatiebeveiliging vaker en met meer diepgang onderwerp van bestuurlijk gesprek tussen departement en taakorganisaties. De gelijke mate van cyberveiligheid krijgt ook concreet vorm door meer gebruik van centraal ingerichte basis ICT-voorzieningen zowel departementaal (Gemeenschappelijke Digitale Diensten) als rijksbreed (Generieke Digitale Infrastructuur) waarop de taakorganisaties hun informatiebeveiliging verder inrichten.

Vraag 8

Hoe vaak en hoe is het iTrechter-systeem gecontroleerd op een mogelijke discriminatoire bias? Kunt u deze analyse(s) met de Kamer delen?

Antwoord

Het iTrechter-systsem is in het verleden niet gecontroleerd op een mogelijke discriminatoire basis. De politie heeft de volgende maatregelen getroffen: het doel van ieder algoritme wordt beschreven in een brondocument, de officier van Justitie toetst de totstandkoming van een algoritme, vooraf aan het activeren van het algoritme wordt er getest of de drempelwaarden juist zijn ingesteld, het algoritme wordt voortdurend aangepast op (onbedoelde) uitzonderingssituaties, er zijn korte feedbackrondes om onterechte signalen gelijk aan te passen, overleg over- en

onderhoud van algoritmes vindt wekelijks plaats, indien nodig ad-hoc, een signaal afkomstig uit het algoritme geldt niet als voldoende voor een controle, er zijn meerdere akkoorden.

Vraag 9

Hoe wordt de privacy van onschuldige burgers gewaarborgd bij het gebruik van iTrechter?

Antwoord

Vanaf de selectie van het veiligheidsprobleem tot aan de feitelijke interventie is in het systeem en het werkproces rekening gehouden met privacy. ANPR-camera's worden uitsluitend geplaatst onder doelbinding. Dat betekent dat gegevens uit de camera's niet voor een ander doel gebruikt worden dan waarvoor ze zijn ingesteld; data zonder verwerkingsgrondslag worden verwijderd, verwerking vindt plaats onder de bepalingen van de Wet politiegegevens; alleen geautoriseerde personen hebben toegang tot naar personen herleidbare data; er vindt een menselijke/professionele toets plaats tussen uitkomsten van het algoritme en de feitelijke controle op straat.

Vraag 10

Kunt u concreet ingaan op de risico's die als categorie 'midden' of 'hoog' zijn getoetst bij het gebruik van iTrechter? Hoe gaat u deze punten concreet verbeteren?

Antwoord

Mitigerende maatregelen op de risico's die als midden of hoog getoetst zijn, worden meegenomen in de ontwikkeling van het Generieke Sensingplatform (GSP).

Vraag 11

Waarom heeft u voor iTrechter geen gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd? Gaat u dit alsnog doen?

Antwoord

De verplichting voor de uitvoering van een gegevensbeschermingseffectbeoordeling (GEB) in de zin van een verwerking in het kader van de Wpg, indien er waarschijnlijk een hoog risico voor de rechten en vrijheden van personen is, is per 1 mei 2018 in de Wpg geïntroduceerd bij de implementatie van de Richtlijn gegevensbescherming opsporing en vervolging. Aangezien een GEB voorafgaand aan de verwerking moet worden uitgevoerd, was dat voor de iTrechter niet verplicht, want de iTrechter bestond al. Er zal een GEB uitgevoerd worden voor het Generieke Sensingplatform (GSP).

Vraag 12

Bij hoeveel profielen heeft u het gebruiken van persoonsgegevens onvoldoende gemotiveerd?

Antwoord

Er zijn door de Algemene Rekenkamer drie algoritmes (profielen) onderzocht. Voor alle drie geldt dat in het onderliggende brondocument wordt vereist dat de gegevensverwerking voldoet aan de doelbinding. Aanvragers hoeven dit echter voor hun algoritme niet te onderbouwen waarom dit geldt voor hun inzet. De politie past dit aan in het vernieuwde brondocument.

Vraag 13

Hoe gaat u opvolging geven aan de aanbeveling om de werkwijze uit te breiden om privacyrisico’s te beperken? Wat is hiervoor uw tijdlijn?

Antwoord

iTrechterfunctionaliteit wordt overgeheveld naar het Generieke Sensingplatform. Aanbevelingen uit het verantwoordingsonderzoek zullen worden meegenomen in de ontwikkeling van dit nieuwe platform.

Vraag 14

Waarom kon u de Algemene Rekenkamer geen inzage geven in de beveiliging van iTrechter? Kunt u dit inzicht in het vervolg alsnog verlenen?

Antwoord

De Algemene Rekenkamer (ARK) heeft, zonder enige belemmering, inzage gehad in de gehele IT-infrastructuur (incl. beveiligingscomponenten) van de iTrechter tijdens haar onderzoek.

De ARK heeft bij deelonderdeel 4.09 'Security by design' van het toetsingskader aangegeven dat als gevolg van een verouderde omgeving niet kan worden aangetoond dat de principes van security by design destijds zijn toegepast. Inzage hierover is niet mogelijk omdat het systeem vijftien jaar oud is. Er valt op basis van de huidige informatie niet aan te tonen op basis van welke principes het ontwerp heeft plaatsgevonden.

Vragen en antwoorden inzake Resultaten verantwoordingsonderzoek 2025 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (36945-VII-2)

Vraag 15

Welke hersteltermijnen hanteert SSC-ICT om digitale werkplekken na een langdurige verstoring weer beschikbaar te maken voor rijksambtenaren?

Antwoord

SSC-ICT levert haar dienstverlening conform voorwaarden die zijn vastgelegd in een Producten en dienstencatalogus (PDC). Er is sprake van een formele hersteltijd (RTO) van maximaal 16 werkuren.

Voor majeure en complexe verstoringen is vooraf geen hersteltijd af te geven. Dit is afhankelijk van de omstandigheden. Wel is SSC-ICT doende om het herstelproces zodanig te optimaliseren dat de doorlooptijd zo kort mogelijk is.

Vraag 16

Op welke wijze wordt digitale soevereiniteit meegewogen bij de keuze en inrichting van digitale werkplekken binnen de rijksoverheid?

Antwoord

Digitale autonomie en de inzet van Open Source heeft veel aandacht binnen de Rijksoverheid, ook bij de keuze en inrichting van de digitale werkplekken. De overheid volgt sinds 2020 het beleid ‘Open, tenzij-beleid’: software van de overheid moet zoveel mogelijk open source zijn. Voor wat betreft de ‘tenzij’ is aangesloten bij de weigeringsgronden van de Wet Open Overheid. Om overheden te helpen dit te operationaliseren is een afwegingskader gemaakt. De huidige digitale werkplek is op dit moment gebaseerd op Microsoft-componenten die deels of geheel in de cloud draaien. Stapsgewijs vervangen we die componenten door autonome componenten. SSC-ICT, DICTU en DUO hebben de opdracht gekregen om een soevereine digitale werkplek te ontwikkelen. Volgend jaar wil ik de eerste testgebruikers overzetten naar deze soevereine digitale werkplek.

Vraag 17

Hoe reageert u op de constatering dat de digitale werkplekken van het Rijk onvoldoende weerbaar zijn? Welke conclusies verbindt u hier aan?

Antwoord

De Algemene Rekenkamer (ARK) constateert dat SSC-ICT voldoende maatregelen treft om het risico op verstoringen of misbruik te verkleinen. De ARK geeft tevens aan dat een vastgesteld bedrijfscontinuïteitsbeleid en een crisismanagementplan mist, en dat SSC-ICT daardoor risico loopt. Zoals ook door de ARK wordt geconstateerd, werkt SSC-ICT hieraan middels een in 2025 gestart programma t.b.v. bedrijfscontinuïteitsmanagement en crisismanagement en het regelmatig oefenen daarvan. Dit programma heeft hoge prioriteit. Onderdeel van dit programma is het in 2026 uitwerken en oefenen van herstelplannen voor de belangrijkste diensten die SSC-ICT levert.

Vraag 18

Op welke manier is de weerbaarheid van de digitale werkplekken reeds onderzocht? Kunt u de uitkomsten, al dan niet vertrouwelijk, aan de Kamer doen toekomen?

Antwoord

SSC-ICT onderzoekt en test doorlopend de weerbaarheid van de digitale werkplekken door het uitvoeren van risicoanalyses, pentesten en audits. SSC-ICT kan de resultaten van security testen vertrouwelijk delen (via de leeskamer-procedure).

Vraag 19

Welke aanbevelingen of acties uit het Uitvoeringsprogramma Compacte Rijksdienst zijn, 16 jaar na de start, volwaardig geïmplementeerd? Welke niet, en waarom niet?

Antwoord

Hiervoor verwijs ik u naar de Jaarrapportage Bedrijfsvoering (JBR) 2014.[1] Het programma Compacte Rijksdienst is eind 2014 door het kabinet afgesloten. Twaalf van de 17 projecten waren op dat moment afgesloten en de resultaten opgeleverd en gemeld via de JBR 2014. De resterende vijf projecten die toen conform planning langer doorliepen zijn in de lijn belegd.

Vraag 20

Waarom is destijds door Economische Zaken besloten om toch eigen digitale werkplekken te ontwikkelen? Wat is het voordeel van de twee digitale werkplekken naast elkaar laten bestaan?

Antwoord

Dit vraagstuk speelde in 2014. Het ministerie van Economische Zaken zou gaan aansluiten bij de digitale werkplek van BZK/SSC-ICT, daarover waren bestuurlijk afspraken gemaakt. SSC-ICT had in die tijd echter geen gelegenheid om een ministerie van de omvang van

---

1 https://open.overheid.nl/overheid/openbaarmakingen/api/v0/attachment/ronl-archief-b2320711-dc7b-4f4c-b0a5-c538846743d9

Economische Zaken, met ruim 12.000 werkplekken (inclusief uitvoeringsorganisaties) te bedienen. Economische Zaken moest destijds een vervanging regelen voor het aflopende werkplekcontract met Capgemini, en kon niet wachten totdat SSC-ICT wel tijd had. Vanwege dit planningsprobleem heeft Economische Zaken besloten toch zelf een digitale werkplek in de markt te zetten. Dit was noodzakelijk voor de continuïteit op dat moment.

Wat verder een rol speelde was dat Economische Zaken ook een aantal uitvoeringsorganisaties bedient (RVO, NVWA) die hogere eisen stellen aan een digitale werkplek dan het gemiddelde kerndepartement. Denk daarbij aan de verwerking van geografische informatie en het mobiel ondersteunen van inspecties in het veld. De digitale werkplek van Economische Zaken biedt daar wel mogelijkheden voor, die de SSC-ICT-werkplek destijds niet bood. Een voordeel hiervan is dat de onderlinge informatie-uitwisseling tussen de uitvoeringsorganisaties en de kerndepartementen beter is geborgd.

Vraag 21

Waarom hebben Algemene Zaken, Defensie, en Onderwijs, Cultuur & Wetenschap hun eigen werkplekvoorziening?

Antwoord

De keuze voor de eigen werkplekvoorziening is een departementale verantwoordelijkheid. Zeven departementen hebben besloten om hun werkplek bij SSC-ICT af te nemen, twee departementen nemen hun werkplek af bij DICTU. Drie departementen hebben besloten om een eigen werkplekvoorziening in te richten. Er is geen inzicht in de beweegredenen van deze departementen om een eigen werkplekvoorziening te gebruiken. Zoals eerder genoemd bij vraag 16, is er wel een initiatief gestart om de werkplekken bij drie dienstverleners te harmoniseren. SSC-ICT, DICTU en DUO hebben de opdracht gekregen om een soevereine digitale werkplek te ontwikkelen. Daarmee worden stappen gezet om een uniforme werkplek aan te bieden aan tien departementen.

Vraag 22

Welke afwegingen maken de verschillende departementen om te kiezen voor 1) de werkplek van SSC-ICT; 2) de werkplek van DICTU; 3) het inrichten van een eigen werkplek?

Antwoord

Zie het antwoord op vraag 21.

Vraag 23

Zijn er schaalvoordelen voor het samenvoegen van werkplekken tot één centrale, digitaal onafhankelijke werkplek? Zijn deze voordelen onderzocht, en zo ja, kunt u ze met de Kamer delen?

Antwoord

Het samenvoegen van werkplekken tot één centrale, digitaal onafhankelijke werkplek kan schaalvoordelen bieden, voor zover het mogelijk is om daarmee aan alle behoeften van de verschillende overheden te voldoen. In zijn algemeenheid geldt dat schaalvergroting tot spreiding van vaste kosten leidt, hetgeen ten goede komt aan de kostprijs. Schaalvergroting leidt ook tot verdere standaardisering binnen het Rijk en effectiever inzetten van schaars IT personeel. In het kader van een ‘slagvaardige overheid’ heeft schaalvergroting dan ook de nadrukkelijke aandacht van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

Vraag 24

Waarom is er nog geen vervolg gegeven aan het onderzoek naar de samenwerking tussen SSC-ICT en DICTU? Wat zijn de redenen?

Antwoord

Er is inmiddels gestart met een verdiepingsonderzoek naar nadere samenwerking op diverse terreinen. De uitkomsten zijn over enige maanden beschikbaar.

Vraag 25

Welke onderzoeken vinden plaats in het kader van de aangekondigde ‘Digitale Dienst’? Wordt het wel of niet samenvoegen van SSC-ICT en DICTU hier expliciet bij betrokken?

Antwoord

Naar aanleiding van de motie Kathmann c.s.[2] heeft de voormalig staatssecretaris van Koninkrijksrelaties en Digitale Zaken advies gevraagd aan de NDS-Raad over de digitale dienst. Dit advies is op 7 mei jl. ontvangen en wordt betrokken bij het verdere onderzoek naar de rol, het mandaat en de positionering die de dienst zou kunnen krijgen. Hoewel het advies niet direct ingaat op het samenvoegen van dienstverleners, wordt wel aangegeven dat een digitale dienst aandacht moet hebben voor het overheidsbreed ‘programmeren’, namelijk het verbinden van de portfolio’s, capaciteit en implementatieplanning van uitvoeringspartners. Uw Kamer wordt door de Staatsecretaris Digitale Economie en Soevereiniteit nader geïnformeerd over de opvolging van dit advies en de eventuele oprichting van een digitale dienst, waarbij een lerende aanpak centraal staat.

Voorts is de Auditdienst Rijk (ADR) gevraagd een onderzoek te doen naar ICT-dienstverleners in de rijksbrede bedrijfsvoering, als vervolg op Motie Buijsse.[3] Zij zal onderzoeken hoe de samenwerking tussen (enkele) dienstverleners, waaronder SSC-ICT en DICTU, verbeterd kan worden en of samenvoeging van diensten/dienstverleners daarbij voordelen kan bieden. Over de uitkomsten van dit onderzoek wordt uw Kamer in de eerste helft van 2027 geïnformeerd. Ook wordt vanuit de rijksorganisatie zelf gekeken hoe een verdere harmonisatie van de dienstverleners eruit zou kunnen zien. Op basis van de bevindingen zal worden beoordeeld of bijstelling van de startpositie van de Nederlandse Digitale Dienst noodzakelijk is.

Vraag 26

---

[2] Kamerstuk 26 643, nr. 1405
[3] Kamerstuk 36740-VII, nr. 30

Wanneer komt het onderzoek uit naar autonome cloudvoorzieningen voor SSC-ICT en DICTU? Wat is het doel en de strekking van het onderzoek precies?

Antwoord

SSC-ICT, DICTU en DUO werken nauw samen bij het onderzoeken van de samenwerking op het terrein van een (rijksbrede) soevereine werkomgeving. De opdracht hiervoor wordt momenteel opgesteld in overleg met de ICBR (interdepartementale commissie bedrijfsvoering rijk). Bedoeling is om in 2026 diverse proof of concepts uit te voeren. Op basis hiervan wordt het vervolgtraject bepaald.

Vraag 27

Hoe verklaart u het grote verschil in de jaarlijkse kosten per gebruiker tussen de werkplek van SSC-ICT en DICTU? Hoe kunt u dat verschil kleiner maken?

Antwoord

Uit het onderzoek door de Rekenkamer is geen verklaring gekomen voor dit prijsverschil. DICTU gaat nu zelf in samenwerking met SSC-ICT onderzoek doen om dit tariefverschil te verklaren.

Vraag 28

Wordt er ook gekeken naar het opschalen van bestaande initiatieven voor digitale autonomie, zoals MijnBureau? Waarom gebruiken SSC-ICT en DICTU hun schaal niet om MijnBureau op te schalen?

Antwoord

Bestaande initiatieven voor digitale autonomie zoals MijnBureau en andere Europese initiatieven worden op herbruikbaarheid bezien bij de ontwikkeling van de (Rijksbrede) Soevereine werkomgeving. Zie hiervoor ook de antwoorden op vragen 22 en 26.

Vraag 29

Wat is uw ambitie voor het wel of niet samenvoegen of samen laten werken van SSC-ICT en DICTU? Welke voor- en nadelen zou dat hebben?

Antwoord

Mijn ambitie is gericht op optimale samenwerking tussen ICT-dienstverleners. Dat heeft als voordelen onder meer kostenbeheersing, interoperabiliteit en inzet van schaarse ICT-resources. Het samenvoegen van ICT-dienstverleners leidt af van de grote opgaven waarvoor het Rijk momenteel is gesteld. SSC-ICT en DICTU, twee van de grootste ICT-dienstverleners binnen het Rijk, werken al op diverse terreinen samen.

Zo lopen er (vervolg)onderzoeken naar nadere samenwerking op het terrein van Oracle en werkplekken en gaan beide organisaties samen met DUO SSC-ICT, in opdracht van de ICBR (interdepartementale commissie bedrijfsvoering rijk) aan de slag met het ontwikkelen van een soevereine werkomgeving. Dit wordt momenteel verder uitgewerkt in een opdracht van de ICBR. Zie ook het antwoord op vraag 26.

Vraag 30

Kunt u de gebruikstarieven voor SSC-ICT en DICTU uiteenzetten? Waar worden die 1.500 / 3.000 euro per werkplek aan uitgegeven?

Antwoord

De tarieven zijn gebaseerd op de kosten die worden gemaakt voor de levering van dienstverlening waaronder personeel, huisvesting, licenties, hardware etc.

Vraag 31

Kunt u alle geconstateerde onrechtmatigheden bij Logius, SSC-ICT en RvIG één-voor-één toelichten?

Antwoord

Hieronder staat een toelichting op de grootste onrechtmatigheden bij Logius, SSC-ICT en RvIG. De resterende onrechtmatigheden zijn relatief beperkt in financiële omvang. Deze zijn bijvoorbeeld ontstaan door foutieve inhuurprocedures, het niet goed doorlopen van een aanbestedingsprocedure voor producten of diensten, of onrechtmatigheden als gevolg van rijksbrede (overbruggings)overeenkomsten van categoriemanagement (deze laatste betreffen in totaal circa € 2,5 mln. voor Logius, SSC-ICT en RvIG).

Logius: totaal circa € 80,5 mln.

- Infrastructuurovereenkomst: circa € 38,6 mln. door gebruik van een onrechtmatige overeenkomst. In 2025 zijn een aantal migraties naar de nieuwe infrastructuur afgerond, waardoor deze onrechtmatigheid in 2026 zal afnemen.
- DigiD en DigiD-machtigen: circa € 15,5 mln. door verlenging van de overeenkomst in 2024. In 2025 is een nieuwe rechtmatige overeenkomst gesloten, waardoor deze onrechtmatigheid per 2026 vervalt.
- Digipoort en Globe: circa € 24,8 mln. door voortgezet gebruik van een onrechtmatige overeenkomst.

SSC-ICT: totaal circa € 55,7 mln.

- Overschrijding van de maximale contractwaarde van ICT-hardware overeenkomsten: circa € 38,5 mln. door onvoldoende monitoring van afnames, gestegen prijzen en hogere afnames dan vooraf ingeschat.
- Bestellingen onder verlopen overeenkomst: circa € 12,5 mln., waarvan circa € 4 mln. het gevolg is van de door de Auditdienst Rijk (ADR) gehanteerde extrapolatiemethode als gevolg van een steekproefcontrole.
- Prestatieonderbouwing bij factuurbetalingen: circa € 3,3 mln. door ontbrekende of onvoldoende kwaliteit van de onderbouwing in de administratie.

Rijksdienst voor Identiteitsgegevens (RvIG): totaal circa € 20,5 mln.

- Berichtendiensten GBA en reisdocumenten: circa € 16,3 mln. door een rechtstreeks en tijdelijk gesloten overeenkomst. RvIG is bezig met het onderbrengen van deze dienstverlening in eigen beheer waarna dit tijdelijke onrechtmatige contract vervalt.
- Siem/SOC-dienstverlening: circa € 1,2 mln. Siem/SOC-dienstverlenging als overbrugging voor het inbesteden van deze dienstverlening.

Voor een uitgebreidere toelichting wordt u verwezen naar de Bedrijfsvoeringsparagraaf in Jaarverslag en Slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2025[4].

Vraag 32

Hoe reageert u op de constatering dat de aanbestedingswetgeving niet wordt nageleefd? Op welke vlakken is dit het geval geweest?

Antwoord

Allereerst zet het ministerie van Binnenlandse Zaken zich in om de aanbestedingsregelgeving na te leven. Alleen in hoogst uitzonderlijke gevallen vindt een afweging plaats tussen rechtmatigheid en doelmatigheid, waarbij vanwege bijvoorbeeld continuïteit- en of veiligheidsredenen op gemandateerd niveau kan worden besloten een onrechtmatige inkoop te doen. Daarnaast kunnen in de controles van controlerende instanties ook rechtmatigheidsfouten worden gerapporteerd. In beide gevallen stuur ik op het voorkomen en ten minste verminderen van deze fouten. Dit doe ik door daarvoor op bestuurlijk niveau binnen het departement aandacht te blijven vragen en het gesprek daarover te blijven voeren, waarbij ook continuïteitsbelangen worden meegewogen.

In het antwoord op vraag 31 leest u op welke vlakken het niet voldoen aan aanbestedingsregelgeving onder meer het geval is geweest.

[4] Kamerstuk Tweede Kamer, vergaderjaar 2025–2026, 36 945 VII, nr. 1

Vraag 33

Wordt / worden er door het niet naleven van de aanbestedingswetgeving één of meerdere marktpartijen bevoordeeld? Kunt u onderbouwen dat hier géén sprake van is?

Antwoord

Het valt niet uit te sluiten dat marktpartijen een voordeel hebben wanneer rechtstreeks een contract wordt gesloten of een overeenkomst onrechtmatig wordt verlengd.

Vragen en antwoorden inzake Resultaten verantwoordingsonderzoek 2025 bij het Ministerie van Economische Zaken (36945-XIII-2)

Vraag 34

Welke aanbevelingen of acties uit het Uitvoeringsprogramma Compacte Rijksdienst zijn, 16 jaar na de start, volwaardig geïmplementeerd? Welke niet, en waarom niet?

Antwoord

Zie vraag 19.

Vraag 35

Kunt u de technische verschillen tussen de werkplekken van SSC-ICT en DICTU, die volgens de Rekenkamer sinds 2023 toenemen, verklaren? Op welke specifieke technische functies verschillen de werkplekken en waarom?

Antwoord

De grootste functionele verschillen bevinden zich op het gebied van opslag en standaardfunctionaliteiten. De opslag voor een gebruiker is bij DICTU ruimer en bij SSC-ICT zijn meer functionaliteiten ‘standaard’. De ‘Digitale Werkomgeving’ van SSC ICT blijft nagenoeg volledig on premise gehost. De ‘Cloud Werkplek’ van DICTU daarentegen maakt gebruik van een deel van de public

clouddiensten van Microsoft. De belangrijkste public cloudapplicaties die DICTU inzet zijn Teams, OneDrive en Exchange Online.

Vraag 36

Wanneer wordt het onderzoek naar een open source cloudplatform afgerond? Hoe worden de uitkomsten gebruikt voor nieuw beleid?

Antwoord

Er heeft een eerste technisch onderzoek plaatsgevonden naar mogelijkheden en toepasselijkheid. Dit is recent met positief resultaat afgerond en biedt houvast voor een functioneel vervolgonderzoek. EZK en BZK bezien komende tijd nader hoe de uitkomsten kunnen worden toegepast in nieuw beleid.

Vraag 37

Kunt u de tariefverschillen tussen de werkplekken van SSC-ICT en DICTU verklaren?

Antwoord

Zie vraag 27.