Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

36 915 VI Wijziging van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2026 (wijziging samenhangende met de Voorjaarsnota)

36 915 XIII Wijziging van de begrotingsstaten van het Ministerie van Economische Zaken (XIII) voor het jaar 2026 (wijziging samenhangende met de Voorjaarsnota)

36 915 VII Wijziging van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2026 (wijziging samenhangende met de Voorjaarsnota)

Nr. 3

VERSLAG HOUDENDE EEN LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 21 april 2026

De vaste commissie voor Digitale Zaken, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer verslag uit te brengen in de vorm van een lijst van vragen met de daarop gegeven antwoorden, over de wijziging van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2026 (wijziging samenhangende met de Voorjaarsnota, Kamerstuk 36 915 VI), wijziging van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) het jaar 2026 (wijziging samenhangende met de Voorjaarsnota, Kamerstuk 36 915 VII), wijziging van de begrotingsstaten van het Ministerie van Economische Zaken voor het jaar 2026 (Wijziging samenhangende met de Voorjaarsnota, Kamerstuk 36 915 XIII), voor zover het onderwerpen betreft die zien op digitalisering.

De vragen zijn op 9 april 2026 voorgelegd aan de Minister van Economische Zaken. Bij brief van 20 april 2026 zijn ze door de Minister van Economische Zaken beantwoord.

kst-36915-VI-3
ISSN 0921 - 7371
's-Gravenhage 2026

Met de vaststelling van het verslag acht de commissie de openbare behandeling van het wetsvoorstel voldoende voorbereid.

De voorzitter van de commissie,
Dekker

Adjunct-griffier van de commissie,
Muller

Vraag 1
Welke structurele overhevelingen van cyberbudgetten zijn vanaf 2027 voorzien vanuit de departementen BZK, FIN, IenW, EZK, LVVN en KGG aan het Nationaal Cyber Security Centrum (NCSC) voor de uitvoering van taken in het kader van de NIS2-richtlijn/Cyberbeveiligingswet (Cbw)?

Antwoord
Tot en met 2027 ontvangt het Nationaal Cyber Security Centrum (NCSC) incidentele middelen van de departementen ten behoeve van de uitvoering van bovengenoemde taken. In 2027 vindt een financiële verdeelsleutelevaluatie plaats. De uitkomsten van deze evaluatie vormen de basis voor de overheveling van middelen vanaf 2028 vanuit de departementen aan het NCSC. Onderdeel van deze evaluatie is dat er wordt gekeken of de opdrachtgevers de middelen na de evaluatie al dan niet structureel zullen overboeken.

Vraag 2
Kan het kabinet toelichten waarom middelen van het Digital Trust Center worden overgeheveld naar het NCSC, welke taken daarmee verschuiven, en hoe wordt geborgd dat de ondersteuning van bedrijven op het gebied van digitale weerbaarheid ten minste op hetzelfde niveau blijft?

Antwoord
De directeur van het Nationaal Cyber Security Centrum (NCSC) is door mij gemachtigd om de wettelijke taken voortvloeiend uit de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) uit te voeren. Deze taken en bevoegdheden werden tot en met 31 december 2025 onder EZK uitgevoerd door het Digital Trust Center (DTC). Het DTC is per 1 januari 2026 samen gegaan met het NCSC tot één versterkt NCSC om zo één overheidsloket voor cybersecurity te creëren voor alle Nederlandse organisaties. Dit samengaan is ook opgenomen in de Nederlandse Cybersecuritystrategie 2022–2028. Bij een departementale herindeling gaan mensen én middelen over naar de ontvangende organisatie. Daarom worden de bijbehorende middelen van het DTC deels structureel en deels jaarlijks naar het NCSC overgeboekt. De structurele middelen worden ingezet voor de financiering van personele capaciteit, ICT-kosten, website (inclusief contentontwikkeling), community en notificatiedienst. Daarnaast worden incidentele middelen ingezet voor o.a. campagnes, netwerkbijeenkomsten en onderzoek. De genoemde integratie met het DTC en de invoering van de Cyberbeveiligingswet (Cbw) beogen tevens de slagkracht van het NCSC te verhogen en zo de digitale weerbaarheid van álle organisaties in Nederland te versterken.

Vraag 3
Waarom zijn de middelen voor de sectorale CSIRT-taken van het NCSC in het kader van de NIS2-richtlijn en de Cbw opgenomen in de begroting van Justitie en Veiligheid maar eindigt het budget na 2027?

Antwoord
Zie vraag 1. Tot en met 2027 ontvangt het Nationaal Cyber Security Centrum (NCSC) incidentele middelen van de departementen ten behoeve van de uitvoering van bovengenoemde taken. In 2027 vindt een financiële verdeelsleutelevaluatie plaats. De uitkomsten van deze evaluatie vormen de basis voor de overheveling van middelen vanaf 2028 vanuit de departementen aan het NCSC. Onderdeel van deze evaluatie is dat er wordt gekeken of de opdrachtgevers de middelen na de evaluatie al dan niet meerjarig oftewel structureel zullen overboeken.

Vraag 4

Kan worden toegelicht welke activiteiten, fte, ICT-systemen, contracten en uitvoeringskosten met de overboeking van het Digital Trust Center naar het Nationaal Cyber Security Centrum overgaan, welk budget en welke taken bij het Digital Trust Center achterblijven en hoe de dienstverlening aan niet-vitale bedrijven vanaf 2026 wordt ingericht?

Antwoord
Ik heb de directeur van het Nationaal Cyber Security Centrum (NCSC) gemachtigd de volgende feitelijke taken uit te voeren (niet uitsluitend): analyseren van dreigings- en incidentinformatie; het opstellen van berichten en het sturen van informatie hierover, waaronder notificaties naar niet-vitale bedrijven; en het contact- en relatiebeheer, waaronder het organiseren van bijeenkomsten met niet-vitale bedrijven. Ook zal het NCSC de volgende diensten verzorgen: website en community, notificatiediensten en ondersteunen samenwerkingsverbanden. Met de departementale herindeling gaat 22,78 fte gepaard. De ICT-ondersteuning voor het DTC en de daarmee gepaard gaande contracten zijn door het Ministerie van Justitie en Veiligheid overgenomen.

Voor de uitvoeringskosten is de volgende verdeling afgesproken:
- structureel overboeken van 5,7 mln. euro (4,8 mln. euro eenmalig in 2026) voor reguliere activiteiten DTC (w.o. website, Community, notificatiedienst),
- jaarlijks overboeken van 1,4 mln. euro voor incidentele/ jaarlijkse activiteiten (w.o. campagnes, netwerkbijeenkomsten en onderzoeken).

Wat achterblijft bij het Ministerie van EZK als beleidsvoorbereidend werk zijn de twee subsidieregelingen van het DTC («Mijn cyberweerbare zaak» en «Versterken cyberweerbaarheid») met een bedrag ter hoogte van 1,9 mln. euro per jaar (subsidiegelden en uitvoeringskosten).

Het Ministerie van EZK blijft opdrachtverstrekker voor de uitvoering voor de taken voortvloeiend uit de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) ten behoeve van het niet-vitale bedrijfsleven.

Vraag 5
Welke budgettaire gevolgen heeft het overhevelen van het digitaliseringsbeleid naar het Ministerie van Economische Zaken gehad voor de begroting van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de capaciteit binnen dit ministerie? Kunt u dit ook uitdrukken in fte?

Antwoord
Op dit moment worden gezamenlijk door de Ministeries BZK en EZK de bestuurlijke en organisatorische wijzigingen naar aanleiding van de portefeuilleherverdeling tussen de Staatssecretaris Digitale Economie en Soevereiniteit en de Staatssecretaris Koninkrijksrelaties en Slagvaardige overheid in kaart gebracht. Hiervoor zijn op beide departementen kwartiermakers aangesteld. Het splitsen van de dossiers binnen het digitaliseringsbeleid vergt uitzoekwerk en kost daarmee tijd. Dit geldt ook voor de bijbehorende capaciteit (fte's) op die dossiers. Uiteraard wordt de medezeggenschap vanuit beide departementen hierbij nauw betrokken. De budgettaire gevolgen van de portefeuille herverdeling worden zichtbaar in de ontwerpbegrotingen voor 2027 van EZK en BZK.

Vraag 6
Welke budgetten worden beheerd of gecoördineerd door de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties? Is er budget dat specifiek aan hem is toegekend?

Antwoord
Budgetten behorende bij het digitaliseringsdossier die voor de herverdeling van portefeuilles onder verantwoordelijkheid vielen van de Staatssecretaris van BZK staan op dit moment nog op de begroting van BZK en zullen waar dat van toepassing is in de Ontwerpbegroting 2027 overgeheveld worden naar EZK.

Vraag 7
Kunt u meer inzicht geven in de meeruitgaven aan de post Adviescollege ICT-toetsing (van € 0 naar € 130.000)?

Antwoord
Dit zijn geen meeruitgaven, maar een verschuiving van middelen van H7 artikel 11 naar H7 artikel 7. Dit zijn middelen die bedoeld zijn voor diverse ICT-onderzoeken. Het Adviescollege ICT-toetsing wordt op de begroting in beginsel verantwoord op artikel 11. Om middelen via het juiste instrument (Opdrachten) uit te kunnen geven, worden deze gealloceerd.

Vraag 8
Kan een integrale tabel worden gegeven van alle uitgaven, overboekingen, kasschuiven, taakstellingen en ontvangsten in 2026 t/m 2031 die direct samenhangen met digitalisering, cyberveiligheid, digitale infrastructuur en informatiehuishouding, uitgesplitst naar begrotingshoofdstuk, artikel, instrument, uitvoerder en juridisch verplicht/bestuurlijk gebonden/vrije ruimte (zie Kamerstuk/bladzijde: 36 915 VII, nr. 2, art. 6 en 7, p. 17–24; 36 915 XIII, nr. 2, art. 1 en 2, p. 10–20; 36 915 VI, nr. 2, art. 36, 91 en 92, p. 22–27)?

Antwoord
We begrijpen de wens om gedetailleerd inzicht te krijgen in de digitaliseringsuitgaven. Hierover zijn door Uw Kamer al meermaals moties aangenomen. In 2024 heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties u middels verschillende brieven[1] hierover geïnformeerd. Hierbij is aangegeven dat er wordt in gezet op het aanvullen en verrijken van de informatie op het Rijks ICT-dashboard en in de Jaarrapportage Bedrijfsvoering Rijk zodat een integraal overzicht weergegeven wordt

Vraag 9
Kan het kabinet een volledige uitsplitsing geven van de reallocatie van het Vernieuwingsbudget van de Generieke Digitale Infrastructuur, inclusief de verschuiving van circa € 64,3 mln. vanuit «Doorontwikkeling en innovatie», naar subsidies, bijdragen aan ZBO's/RWT's, medeoverheden, agentschappen en overige bijdragen, met per onderdeel het project, het bedrag en het beoogde resultaat (zie Kamerstuk/bladzijde: 36 915 VII, nr. 2, art. 6.8 Generieke Digitale Infrastructuur, p. 17–20)?

Antwoord
Ik verwijs hiervoor naar het GDI programmeringsplan 2026, dat eerder met de Kamer is gedeeld als bijlage bij de Verzamelbrief Digitalisering december 2025[2]. In dit programmeringsplan zijn per project de middelen, de toedeling en de beoogde resultaten opgenomen. Hieronder is een uitsplitsing opgenomen naar subsidies, bijdragen aan ZBO's/RWT's, medeoverheden, agentschappen en overige bijdragen. Onderstaande uitsplitsing is eerder opgesteld dan de 1e suppletoire begroting en geeft een totaalbeeld weer van de programma's onder de GDI.

[1] TZ202411-102 en Kamerstuknummer II, 2024/25, 36 740 VII, nr. 29
[2] Kamerstuknummer II, 2025/26, 26 643, nr. 1450

Uitsplitsing van de verschuivingen:

Subsidies	
Dossier	bedrag x € 1.000
Gebruik van Europese componenten uit de Digital Decade in de GDI	3.796
Innovatiewerkplaats Digilab	2.034
Uit betrouwbare bron (UBB) – voorheen Data bij de bron	1.442
Standaard methodiek toegangsverlening tot data	473
Digitaal dossier overheidsbrede dienstverlening	968
Portaal Caribisch Nederland	224
Innovatiebudgetbudget 2026	600
Diverse overlopende verplichtingen	900

Bijdragen aan ZBO's/RWT's	
KVK	bedrag x € 1.000
Beheer Digitaal ondernemersplein	6.621
ICTU	
Algemene Bijdrage Digicampus	320
Implementatie SDG-Fase 2: Procedures en Once Only technical System	608
Implementatie Stelsel Toegang	2.000
Europese Raamwerk voor Digitale Identiteitswallets: Europese large scale pilots	1.600
Europese Raamwerk voor Digitale Identiteitswallets: Programma EDI-stelsel NL	3.260
Innovatiebudgetbudget 2026	3.500
GDI monitor 2026 Aansluit potentieel GDI	160
RDW	
PGDI Implementatieondersteuning en Kennisborging	1.200
Diverse bijdragen	
Europese Raamwerk voor Digitale Identiteitswallets: Programma EDI-stelsel NL en Europese large scale pilots	400
Beheer: Toezicht eProcurement RDI	668
Medeoverheden	
Het innovatiebudget verstrekt bijdragen aan medeoverheden voor het uitvoeren van innovatieve projecten. Dit bedrag wordt nader bepaald in 2026 bij de toewijzing van innovatiebudgetten en is daarom nu niet verder te specificeren	

Agentschappen	
Logius	bedrag x € 1.000
Herbouw Digipoort	6.944
Federatief berichten Stelsel (FBS)	11.920
Doorontwikkeling MijnOverheid en overheidsbrede interactieservices	2.500
MijnOverheid voor Ondernemers	1.500
Doorontwikkeling Diginetwerk	640
Overheid.nl als wegwijzer naar informatie en diensten	1.770
RvIG	
Beheer: eIDAS RvIG	7.371
Beheer: BSN RvIG	7.429
RVO	
Berichtenbox Zakelijk	500
D&I: RVO	1.497
Algemeen – Diverse bijdragen onder agentschappen	
DICTU onderdeel van Stelsel Toegang	1.920

Vraag 10
Kan het kabinet per project toelichten welke concrete prestaties in 2026 worden geleverd met de subsidies en bijdragen voor onder andere de VNG, ICTU, Logius, Digilab, het Europese raamwerk voor digitale identiteitswallets, Stelsel Toegang, Herbouw Digipoort en het Federatief Berichtenstelsel (zie Kamerstuk/bladzijde: 36 915 VII, nr. 2, art. 6.8, p. 17–20)?

Antwoord
Ik verwijs hiervoor naar het GDI programmeringsplan 2026, dat eerder met de Kamer is gedeeld als bijlage bij de Verzamelbrief Digitalisering december 2025[3]. In dit programmeringsplan zijn per project de resultaten, activiteiten en bijbehorende middelen opgenomen. Daarmee bevat het document de gevraagde toelichting op de prestaties die in 2026 worden gerealiseerd met de subsidies en bijdragen aan onder meer VNG, ICTU, Logius, Digilab, het Europese raamwerk voor digitale identiteitswallets, Stelsel Toegang, Herbouw Digipoort en het Federatief Berichtenstelsel.

De relevante projectbeschrijvingen zijn te vinden op de volgende pagina's van het GDI-programmeringsplan 2026:
- Digilab – p. 39
- Europees raamwerk voor digitale identiteitswallets – p. 44
- Stelsel Toegang – p. 44
- Herbouw Digipoort – p. 41
- Federatief Berichtenstelsel – p. 41

Vraag 11
Kan het kabinet uitsplitsen hoe de post «Diensten en producten uitvoeringsorganisaties» van € 155,4 mln. in 2026 is verdeeld over de Rijksorganisatie voor Informatiehuishouding, Rijksinkoopsamenwerking en Organisatie voor Bedrijfsvoering en Financiën, en welk deel daarvan betrekking heeft op digitale taken, informatiehuishouding en ICT-dienstverlening (zie Kamerstuk/bladzijde: 36 915 VII, nr. 2, tabel 2 en art. 11, p. 5–11 en 35–42)?

Antwoord
De 155,4 mln. euro is als volgt verdeeld over de Rijksorganisatie voor Informatiehuishouding (RvIHH), Rijksinkoopsamenwerking (RIS) en Organisatie voor Bedrijfsvoering en Financiën (OBF):

	Bedragen x € 1.000
RvIHH	102.085
RIS	24.648
OBF	28.676
Totaal	155.409

Binnen deze begrotingen zijn de volgende budgetten geraamd onder het instrument ICT (materiële uitgaven):

	Bedragen x € 1.000
RvIHH	20.959
RIS	955
OBF	6.931
Totaal	28.845

Graag informeren we de Kamer over de verdere uitsplitsing in een brief die op een later moment volgt.

Vraag 12
Zijn er aanvullende middelen vrijgemaakt voor de Informatiepunten Digitale Overheid ter uitvoering van de gewijzigde motie-Kathmann (Kamerstuk 36 740 VII, nr. 35)?

[3] Kamerstuknummer II, 2025/26, 26 643, nr. 1450

Antwoord
Bij de 1e suppletoire begroting 2026 zijn middelen beschikbaar gesteld ten behoeve van het terugdraaien van de eerder doorgevoerde 10% budgetkorting op de specifieke uitkering Informatiepunten Digitale Overheid. Deze middelen zijn grotendeels afkomstig vanuit de Aanvullende Post vanuit de reservering naar aanleiding van de Parlementaire Onderzoekscommissie Kinderopvangtoeslag (1,3 mln. euro in 2026 en vanaf 2027 structureel 1,7 mln. euro) en deels vanaf het artikel 6.2 Overheidsdienstverlening, informatiebeleid en informatiesamenleving (0,4 mln. euro in 2026 en vanaf 2027 structureel 0,01 mln. euro). De middelen zijn bij de 1e suppletoire begroting 2026 overgeheveld naar het Gemeentefonds. Op deze wijze wordt er uitvoering gegeven aan de gewijzigde motie-Kathmann (GL-PvdA)[4].

Vraag 13
Welke middelen zijn er beschikbaar voor het uitvoeren van de Nederlandse Digitaliseringsstrategie? Wordt dit (t.z.t.) deels bekostigd uit de begroting van het Ministerie van Economische Zaken?

Antwoord
Voor de Nederlandse Digitaliseringsstrategie[5] zijn geen aanvullende budgetten – budgetten anders dan reeds beschikbare middelen op de BZK-begroting die binnen de scope van de NDS vallen – opgenomen in de begroting van 2026. Vanuit het coalitieakkoord is ook geen nader budget beschikbaar gesteld op de begroting van Economische Zaken en Klimaat voor het domein digitalisering.

Vraag 14
Welke budgetten worden beheerd of gecoördineerd door de Staatssecretaris van Economische Zaken en Klimaat? Is er budget dat specifiek aan haar is toegekend voor digitaliseringsbeleid?

Antwoord
Op dit moment wordt aan de bestuurlijke en organisatorische veranderingen tussen BZK en EZK gewerkt, hieronder vallen ook de budgetten. In de begrotingen voor 2027 zal dit budgettair worden verwerkt.

Vraag 15
Welke budgettaire gevolgen zijn er voor de uitvoering van de motie-Kathmann (Kamerstuk 26 643-1316) over het aanbesteden van een Rijkscloud? Welke kosten worden er voorzien?

Antwoord
Zoals eerder met de Kamer gedeeld, werken we op dit moment aan de verkenning van de soevereine overheidscloud. Op basis van die verkenning volgt een voorkeursscenario dat nader uitgewerkt gaat worden. Aanbesteden is één van de scenario's die in de verkenning wordt bekeken. Het uitwerken van een raming van het voorkeursscenario is een volgende stap.

Vraag 16
Welke middelen zijn er beschikbaar voor publieke investeringen in digitale infrastructuur, zoals zeekabels en rekenkracht? Uit welke budgetten worden de ambities voor digitale autonomie op termijn bekostigd?

Antwoord

[4] Kamerstuknummer II, 2025/26 36 740 VII, nr. 35
[5] Kamerstuknummer II, 2024/25, 26 643, nr. 1336

Op dit moment vindt nog nadere interdepartementale afstemming plaats over de wijze waarop de ambities ten aanzien van digitale autonomie op termijn kunnen worden gefinancierd.

Investeringen in digitale infrastructuur zijn namelijk overwegend privaat. De overheid zorgt voor de kaders en randvoorwaarden. Hierdoor kunnen marktpartijen investeren, innoveren en is er een hoogwaardig, concurrerend, weerbaar en betaalbaar aanbod met voldoende keuzevrijheid voor gebruikers. Met gegronde redenen kan aanvullende publieke financiering worden ingezet, zoals bijvoorbeeld voor de AI-fabriek (132 mln. euro, naast circa 71 mln. euro vanuit EuroHPC) en het NGF-project 6G Future Network Services (203 mln. euro). Ook kan de overheid met eigen aanbestedingen van digitale dienstverlening, zoals cloudtechnologie, het Europese marktaanbod stimuleren.

Voor aanvullende investeringen zoals nieuwe strategische zeekabels is op dit moment geen budget gereserveerd op de begroting van EZK. Eventuele besluitvorming hierover kan daarom pas worden betrokken bij een volgend budgettair besluitvormingsmoment. Vanaf Q3 2026 zal het kabinet uw Kamer informeren over intercontinentale zeekabels. Publieke investeringen voor de realisatie van rekenkracht voor onderzoek en onderwijs vallen onder de verantwoordelijkheid van het Ministerie van Onderwijs, Cultuur en Wetenschap.

Vraag 17
Wat is de reden dat de toegezegde middelen voor het stimuleren van cyberinnovatie op de begroting van EZK niet terug te vinden zijn in de Voorjaarsnota en de suppletoire begroting?

Antwoord
Voor het stimuleren van cybersecurity innovatie is 4 mln. euro per jaar tot 2028 beschikbaar op de EZK-begroting. Deze middelen leveren een bijdrage aan het realiseren van pijler II «Veilige en innovatieve digitale producten en diensten» van de Nederlandse Cybersecuritystrategie 2022–2028[6]. Deze middelen zijn te vinden in het totaalbedrag onder Cyber security. Deze middelen zijn niet terug te vinden in de Voorjaarsnota en eerste suppletoire begroting omdat die toezien op wijzigingen in de begrotingen die in het voorjaar hebben plaatsgevonden.

Vraag 18
Kan het kabinet toelichten waarom de overboekingen voor de NGF-projecten «6G Future Network Services» in 2027 hoger uitvallen in 2027 ten opzichte van 2026 en 2028–2029?

Antwoord
Begin maart zijn de resterende gereserveerde middelen voor het project 6G Future Network Services à 142 mln. euro definitief toegekend. In 2026 zijn de middelen alleen voor de tweede helft van het jaar. Projectactiviteiten in de eerste helft van 2026 worden gefinancierd uit de eerder toegekende NGF-middelen voor fase 1 van het project. In 2027 wordt een piek in de projectactiviteiten verwacht, waardoor de uitgaven in 2027 hoger zijn dan in de jaren daarop. Dat heeft te maken met de planning van de werkzaamheden (onderzoek & innovatie) door het consortium, dat het project uitvoert.

Vraag 19
Kan het kabinet toelichten hoe de kasschuiven voor de Nationaal Groeifonds-projecten (kwantumDelta, Oncode, NXTGEN en PhotonDelta)

[6] Kamerstuknummer II, 2022/23, 26 643, nr. 925

in elkaar zitten? Het budget wordt afgebouwd, maar vervolgens in 2031 weer opgebouwd. Waarom is dit geld specifiek in 2031 wel nodig?

Antwoord
De verschillende NGF-projecten kennen een eigen looptijd in einddatum. Voor trajecten die in de latere rondes zijn toegekend lopen een aantal tot in 2033. Omdat de begrotingssystematiek van de overheid een meerjarenperiode van zes jaar kent, komt het voor dat de middelen voor de projecten die buiten deze periode vallen in het laatste jaar staan. Zo is dat ook hier zo, waardoor zodra er een nieuw jaar beschikbaar is, middelen in het juiste ritme geplaatst kunnen worden.

Vraag 20
Kan het kabinet toelichten waar de middelen voor «Digitale Veiligheid» op de aanvullende post concreet voor bedoeld zijn en welke projecten hiermee worden gefinancierd? Waarom staat een bedrag van 78 mln. op de aanvullende post zonder nadere specificatie? Waarom stopt de financiering in 2026? Kan er een overzicht worden gegeven van de middelen die binnen de envelop voor (nationale) veiligheid worden ingezet voor digitale weerbaarheid, voorbereiding op grootschalige digitale aanvallen, oefeningen met overheid, mkb en vitale sectoren, ondersteuning van ethische hackers, dreigingsinformatie-uitwisseling, digitale handhaving en toezicht op online platforms, met per onderdeel het verantwoordelijke ministerie, de uitvoerder, het begrotingsartikel en het bedrag per jaar 2026 t/m 2031 en structureel?

Antwoord
Gezien de commerciële vertrouwelijkheid die raakt aan de middelen die gereserveerd staan op de post «Digitale Veiligheid» wordt deze niet verder gespecificeerd. De uitgave die wordt voorzien is incidenteel en loopt daarom na 2026 af.
De intensiveringen uit het coalitieakkoord, waaronder de envelop voor (nationale) veiligheid, zijn op de aanvullende post geboekt. De invulling hiervan wordt op het moment uitgewerkt. Inzicht daarin kan daarmee nog niet worden gegeven.

Vraag 21
Wat is uw definitie van digitale soevereiniteit?

Antwoord
In de Agenda Digitale Open Strategische Autonomie[7] is digitale autonomie gedefinieerd als het vermogen van de EU om in het digitale domein als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld. Digitale autonomie komt daarmee in de eerste plaats neer op handelingsvrijheid.
In de Visie Digitale Autonomie en Soevereiniteit[8] van de overheid wordt digitale soevereiniteit beschreven als de mate waarin de overheid zeggenschap en controle heeft over haar digitale infrastructuur, data en systemen, zodat publieke waarden (zoals veiligheid, privacy en democratie) geborgd blijven.
In de praktijk lopen deze begrippen door elkaar heen. Zo wordt op EU-niveau met digitale soevereiniteit soms juist handelingsvrijheid bedoeld. Beleidsmatig is handelingsvrijheid altijd gewenst; eigenaarschap en controle alleen daar waar nodig.

Vraag 22

[7] Kamerstuknummer II, 2023/24, 36 259, nr. 21
[8] Kamerstuknummer II, 2025/26, 26 643, nr. 1450

Wat is uw definitie van online veiligheid?

Antwoord
De huidige doelstellingen geldend in 2026 ten aanzien van (online) veiligheid staan opgenomen in de Veiligheidsagenda 2023–2026. Onderdeel hiervan zijn de doelstellingen ten aanzien van online criminaliteit (cyber en gedigitaliseerde criminaliteit). Met partners in het Landelijk Overleg Veiligheid en Politie wordt gewerkt aan het opstellen van nieuwe doelstellingen voor de Veiligheidsagenda 2027–2030.

Vraag 23
Zijn er concrete doelstellingen (KPI's) geformuleerd voor digitale soevereiniteit in 2026–2030? Zo ja, welke?

Antwoord
In prioriteit vijf «Versterken digitale weerbaarheid en autonomie van de overheid» in de NDS (Nederlandse Digitaliseringsstrategie) is opgenomen dat beleid wordt ontwikkeld om de gezamenlijke digitale autonomie te vergroten. Dit onderwerp wordt onder meer meegenomen in de herziening van het rijksbrede cloudbeleid en in de IT-sourcingstrategie Rijk. Daarnaast wordt momenteel gewerkt aan een routekaart digitale autonomie en soevereiniteit van de overheid, waarin de route naar het verminderen van afhankelijkheden wordt uitgewerkt. In deze routekaart worden ook doelstellingen geformuleerd. De Kamer wordt via de reguliere verzamelbrieven geïnformeerd over de voortgang.
Op Europees niveau hebben de EU-lidstaten zich gecommitteerd aan ambitieuze digitaliseringsdoelstellingen voor 2030 via het Europese Digital Decade beleidsprogramma. Het zorgen voor digitale soevereiniteit van de EU is één van deze doelstellingen. De Digital Decade doelstellingen zijn nader uitgewerkt in specifieke KPI's die ook zijn opgenomen in de Strategie Digitale Economie (SDE)[9].
De KPI's van de SDE dragen bij aan het versterken van de randvoorwaarden voor digitale soevereiniteit. Zo zijn er onder de SDE doelstellingen voor het versterken van digitaal talent en de innovatiekracht van het MKB.

Vraag 24
Zijn er concrete doelstellingen (KPI's) geformuleerd voor online veiligheid in 2026–2030? Zo ja, welke?

Antwoord
Met partners in het Landelijk Overleg Veiligheid en Politie (LOVP) wordt gewerkt aan het opstellen van nieuwe doelstellingen voor de Veiligheidsagenda 2026–2030. Dat geldt ook ten aanzien van online criminaliteit (cyber en gedigitaliseerde criminaliteit)

Vraag 25
Op welke wijze wordt de voortgang op deze doelstellingen gemonitord en aan de Kamer gerapporteerd?

Antwoord
Zie antwoord vraag 23. Ten aanzien van de voortgang van de doelstellingen online criminaliteit wordt jaarlijks gerapporteerd in het Jaarverslag van het Ministerie van JenV en het halfjaarbericht politie.

Vraag 26
Hoe ontwikkelt de verhouding tussen interne digitale expertise en externe ICT-inhuur binnen de rijksoverheid?

[9] Kamerstuknummer II, 2022/23, 26 643, nr. 941

Antwoord
De rijksoverheid is de afgelopen jaren voor digitale expertise relatief sterk afhankelijk geweest van externe ICT-inhuur, mede door arbeidsmarktkrapte en de specialistische aard van ICT-werkzaamheden. Ontwikkelingen die van invloed zijn op de verhouding intern/extern personeel, zijn de taakstelling op intern personeel en het verambtelijken van externe inhuur. Om beter inzicht te krijgen in deze verhouding en de ontwikkeling daarvan, wordt gewerkt aan het verbeteren van de monitoring, onder meer via de invoering van het Kwaliteitsraamwerk Informatievoorziening (KWIV) en het IV-personeelsdashboard. Er wordt gewerkt aan een rijksbrede personeelsstrategie voor digitalisering, waarvan de eerste onderdelen eind 2027 worden opgeleverd. Daarnaast heeft het kabinet de ambitie om specialistische kennis vaker in vaste dienst te nemen in plaats dan in te huren.

Vraag 27
Hoe wordt door u centrale regie gevoerd op de digitaliseringsuitgaven over de Ministeries van BZK, EZK en JenV?

Antwoord
Onderlinge afstemming tussen de drie ministeries vindt op de specifieke domeinen altijd plaats. Wat betreft de nieuwe portefeuille herverdeling wordt op het moment aan de bestuurlijke en organisatorische veranderingen tussen BZK en EZK gewerkt.

Vraag 28
Kunt u een overzicht geven van budgetten voor digitale zaken, inclusief eventuele overlap en versnippering tussen departementen?

Antwoord
Zie antwoord vraag 8.

Vraag 29
Welke onderdelen van de investeringen ten behoeve van het Nationaal Agentschap voor Disruptieve Innovatie (NADI) en de Nationale Investeringsinstelling (NII) worden voorzien van een digitaal oormerk?

Antwoord
De vormgeving van de NADI wordt nog uitgewerkt. Daardoor is er op dit moment nog geen informatie over verschillende oormerken.

Vraag 30
Hoe is de structurele financiering van het Nationaal Cyber Security Centrum (NCSC) vormgegeven?

Antwoord
Het Nationaal Cyber Security Centrum (NCSC) wordt voor een belangrijk deel gefinancierd uit de begroting van JenV. Daarnaast dragen de departementen BZK, FIN, IenW, LVVN, EZK en BUZA als opdrachtgevers van overige (wettelijke) taken bij aan de financiering van het NCSC. Structurele financiering is onderdeel van de evaluatie van de financiële verdeelsleutel die in 2027 plaatsvindt.

Vraag 31
Wat is de stand van zaken van de investeringsagenda binnen de Nederlandse Digitaliseringsstrategie (NDS)?

Antwoord

De stand van zaken investeringsagenda is in november 2025 met uw Kamer gedeeld[10]. Momenteel wordt dit samen met medeoverheden en publieke dienstverleners verder uitgediept om op basis daarvan te bepalen waar we met de NDS op in willen zetten de komende jaren. In de Kamerbrief strategische inzet digitalisering en autonomie zullen de prioritering en bijbehorende beschikbare budgetten op de NDS verder worden toegelicht. Het streven is om deze voor de zomer naar uw Kamer te verzenden.

Vraag 32
Hoe staat het met de uitvoering van de motie-El Boujdaini c.s. (Kamerstuk 36 800 VII-76)?

Antwoord
Vanwege een eerdere toezegging en motie[11] werd er al gewerkt aan een plan om het inzicht in de uitgaven aan digitalisering te verbeteren. Deze motie wordt meegenomen in dat traject. Ik streef ernaar u voor de zomer te informeren over dit plan.

Vraag 33
Worden digitaliseringsprojecten standaard getoetst aan grondrechten en publieke waarden? Zo ja, hoe is dit proces ingericht?

Antwoord
De overheid moet grondrechten beschermen en rekening houden met publieke waarden, ook bij het uitvoeren van digitaliseringsprojecten. Grondrechten zoals het recht op privacy en het verbod op discriminatie zijn verankerd en uitgewerkt in wetgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), Algemene Wet Gelijke Behandeling (AWGB), en de AI-Verordening. Digitaliseringsprojecten, van zowel de overheid als andere organisaties, moeten hieraan voldoen.

Daarnaast kunnen organisaties ook gebruik maken van Nationale en Europese hulpmiddelen zoals de Code Goed Digitaal Openbaar Bestuur (CODIO), Data Protection Impact Assessment (DPIA), de Handreiking aanbesteden van open source software II, of het Impact Assessment Mensenrechten en Algoritmes (IAMA) om de impact van digitaliserings-projecten op grondrechten en publieke waarden in kaart te brengen en, om op basis daarvan, maatregelen te nemen om eventuele risico's te mitigeren.

Vraag 34
Welke concrete waarborgen gelden voor de inzet van AI binnen de overheid?

Antwoord
Het is van belang dat de inzet van AI in lijn is met bestaande wet- en regelgeving zoals het discriminatieverbod, privacywetgeving (rechtmatige verwerking van persoonsgegevens en recht op betekenisvolle menselijke tussenkomst conform de Algemene Verordening Gegevensbescherming (AVG)) of regels omtrent het contact tussen overheid en burgers/bedrijven zoals de algemene beginselen van behoorlijk bestuur (Awb). Vanuit de Europese Unie (EU) zijn er risico-gebaseerde regels die betrekking hebben op de technologie zelf. Deze staan voor AI-systemen vastgelegd in de Europese AI-verordening die vanaf augustus 2024 in werking is getreden. De verschillende onderdelen van de verordening worden sinds februari 2025 stapsgewijs van toepassing. Deze regels gelden voor alle

[10] Kamerstuknummer II, 2025/26, 26 643, nr. 1435
[11] TZ202411-102 en Kamerstuknummer II, 2024/25, 36 740 VII, nr. 29

EU-lidstaten. In de AI-verordening is onder meer een verbod opgenomen voor AI-systemen die manipuleren of misleiden en is er een categorie hoog risico AI die toelaatbaar zijn, maar waarvoor eisen gelden om risico's te mitigeren. Ook gelden voor (overheids)organisaties regels voor transparantie rondom de inzet van (generatieve) AI, zoals chatbots en met AI-gegeneerde afbeeldingen.

Vraag 35
Welke risicoanalyses worden uitgevoerd bij inzet van algoritmen en AI?

Antwoord
Bij de inzet van algoritmen en AI biedt het Algoritmekader een handzaam overzicht van de belangrijkste wet- en regelgeving, inclusief de verplichte en geadviseerde maatregelen om risico's tijdig in kaart te brengen en te mitigeren[12].
Indien bij de inzet van algoritmen en AI-persoonsgegevens worden verwerkt, is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Volgens de AVG is een gegevensbeschermingseffectenbeoordeling (DPIA) verplicht bij een verwerking van persoonsgegevens die gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen.
Hoewel er bij de inzet van algoritmen en AI momenteel nog geen algemene risicoanalyse verplicht is, heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in 2021 het Impact Assessment Mensenrechten en Algoritmen (IAMA) ontwikkeld. Het IAMA is bedoeld om de risico's voor grondrechten bij de inzet van algoritmen en AI door de overheid tijdig te identificeren en te mitigeren; tegelijkertijd zorgt het voor transparantie en publieke verantwoording.
Vanuit Europa wordt vanaf 2 augustus 2026 de Fundamental Rights Impact Assessment (FRIA) verplicht voor publieke organisaties en private organisaties die publieke diensten verlenen bij de inzet van hoog-risico AI-systemen[13]. Een FRIA wordt verplicht voor publieke organisaties en private organisaties die publieke diensten verlenen bij de inzet van hoog-risico AI. Het IAMA is onlangs geactualiseerd en in lijn gebracht met deze FRIA-verplichting[14]. Rijksbreed is afgesproken om het IAMA nu al te gebruiken bij impactvolle algoritmen en hoog-risico AI, vooruitlopend voordat op alle onderdelen van de AI-verordening van toepassing zijn.
In aanvulling op het IAMA zijn er tot slot diverse methoden om verboden of ongewenst onderscheid en discriminatierisico's te bepalen, zoals de handreiking non-discriminatie, het fairness handboek, biastoetsen of het toetsingskader risicoprofilering

Vraag 36
Hoe wordt transparantie van overheidsalgoritmen richting burgers gewaarborgd?

Antwoord
De Staatssecretaris van BZK werkt in algemene zin aan het verbeteren van transparantie van alle algoritmen die overheden gebruiken, onder andere door middel van het algoritmeregister. Binnen de Rijksoverheid zijn afspraken gemaakt over het registreren van alle hoog-risico AI-systemen en impactvolle algoritmen. Over de voortgang hiervan zal uw Kamer via de Jaarrapportage Bedrijfsvoering Rijk (JBR) worden geïnformeerd.

---

[12] https://minbzk.github.io/Algoritmekader/
[13] Artikel 27 AI-verordening
[14] https://www.digitaleoverheid.nl/nieuws/iama-aangepast-aan-praktijk-en-regelgeving/

Verder heb ik de Auditdienst Rijk opdracht gegeven om de kwaliteit van de registraties in het register te onderzoeken.

Daarnaast wordt momenteel door de Staatssecretaris van JenV samen met de Staatssecretaris van BZK en mijzelf een beleidsonderzoek verricht naar de mogelijkheden tot aanpassing van de bestaande normen en definities in de Awb met als doel om meer transparantie en rechtsbescherming te creëren bij algoritmische besluitvorming door de overheid. Hierover is de Kamer bij brief van 11 juli 2025[15] geïnformeerd. Het kabinet streeft ernaar de Kamer hierover uiterlijk in oktober 2026 te informeren.

Aansluitend aan het beleidsonderzoek worden pilots uitgevoerd om de behoeften van burgers voor transparantie bij algoritmen te bepalen, en hoe aan deze behoeften door uitvoerders invulling kan worden gegeven. Dit betreft twee pilots bij de SVB en DUO voor algemene beelden, en drie pilots over Open Algoritmen als onderdeel van het Herijkte Actieplan Open Overheid 2023–2027[16] dat 25 december 2025 naar uw Kamer is gestuurd.

Vraag 37
In welke fase bevindt de BTI-toets met betrekking tot de overname van Solvinity door Kyndryl zich?

Antwoord
Over onderzoeken van BTI worden normaliter geen uitspraken gedaan. Omdat de betrokken bedrijven in dit geval in de media gedeeld hebben dat zij een melding hebben ingediend kan worden bevestigd dat het onderzoek loopt en er nog geen besluit genomen is.

Vraag 38
Hoe staat het met de uitvoering van de motie Six Dijkstra c.s. (Kamerstuk 26 643-1408)?

Antwoord
In een Kamerbrief dd. 9 december 2025[17] is ingegaan op de wijze waarop deze motie uitgevoerd wordt. Op 23 maart jl. heeft uw Kamer tevens schriftelijke vragen gesteld inzake onder meer de status van de uitvoering van deze motie. In de beantwoording op deze Kamervragen zal nader ingegaan worden op de status van deze motie.

Vraag 39
Wanneer verwacht u inzicht te verkrijgen in de gebruikers van de zeven te bouwen megadatacentra?

Antwoord
Er bestaat geen verplichting voor beheerders van datacentra om bij landelijke autoriteiten melding te maken over de doeleinden waarvoor ze een datacentrum gebruiken of over de partijen die in hun datacentrum capaciteit afnemen. Het kabinet heeft daarmee geen andere informatie tot zijn beschikking dan wat in recente mediaberichtgeving is gepubliceerd over de nog te ontwikkelen datacentra.

[15] Kamerstukken II, 2024/25, 26 643, nr. 1372
[16] Bijlage bij Kamerstukken II, 2025/26, 29 362, nr. 393
[17] Kamerstukken II, 2025/26, 26 643, nr. 1441