

36 740 VI Jaarverslag en slotwet Ministerie van Justitie en Veiligheid 2024

36 740 VII Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2024

36 740 XIII Jaarverslag en slotwet Ministerie van Economische Zaken en Klimaat 2024

Nr. 12 VERSLAG HOUDENDE EEN LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 13 juni 2025

De vaste commissie voor Digitale Zaken, belast met het voorbereidend onderzoek van dit voorstel van wet voor zover het onderwerpen betreft die zien op digitalisering, heeft de eer verslag uit te brengen in de vorm van een lijst van vragen met de daarop gegeven antwoorden.

De vragen zijn op 28 mei 2025 voorgelegd aan de minister en staatssecretaris van Justitie en Veiligheid. Bij brief van 6 juni 2025 zijn ze door de minister en staatssecretaris van Justitie en Veiligheid beantwoord.

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

De voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller

Vraag (1):

Welke risico's ziet u bij de implementatie van de e-Justice-, AI- en eIDAS-verordeningen voor nationale IT-autonomie?

Antwoord:

In algemene zin streeft het kabinet naar zogenaamde Europese open strategische autonomie in het digitale domein. Als het gaat om digitale autonomie, is het juist belangrijk om dit in EU-verband te doen en bezien en hier niet nationale autonomie (volledig) leidend te laten zijn. Samenwerking binnen de EU is cruciaal om als mondiale speler, in samenwerking met internationale partners, op basis van eigen inzichten en keuzes onze publieke belangen te borgen, weerbaar te zijn en het concurrentievermogen van Europese (en dus Nederlandse) bedrijven te behouden of zelfs te vergroten.

De AI-verordening zorgt voor geharmoniseerde regels voor verantwoorde en betrouwbare AI op de Europese markt. De AI-verordening is een proportioneel gemeenschappelijk regelgevend kader dat voorkomt dat Europese aanbieders in verschillende landen aan verschillende regels moeten voldoen. Ook (grote) aanbieders van AI uit derde landen moeten aan de eisen uit de AI-verordening voldoen, wat onze (EU-)autonomie vergroot. Tegelijkertijd is het belangrijk dat Europese aanbieders worden ondersteund in het voldoen aan de AI-verordening. Het kabinet zet hier actief op in door het opzetten van regulatory sandboxes en heldere communicatie, zoals de Gids AI-verordening.

Ook vanuit de Europese Unie komt er ondersteuning voor aanbieders via de AI Act Service

Desk. Naast de AI-verordening zet de EU ook actief in op het stimuleren van AI-ontwikkeling binnen de EU. In het recent aangekondigde AI Continent Action Plan heeft de Europese Commissie verschillende maatregelen aangekondigd om data- en computerinfrastructuur te bouwen, toegang tot data te vergroten, AI-talent te versterken en de adoptie van AI in sectoren te stimuleren.

Wat betreft de eIDAS-verordening is het zo dat deze beoogt de afhankelijkheid van Big Tech te verminderen, doordat lidstaten verplicht zijn een wallet uit te geven of te erkennen, die aan de EU-eisen voldoet.

De vertrouwensdiensten in eIDAS maken gebruik van open standaarden die door Europese standaardisatieinstituten zijn opgesteld.

Doel van de e-Justice-verordening¹ [1] is het vergemakkelijken van grensoverschrijdende communicatie tussen justitiële autoriteiten²

¹ Voluit: VERORDENING (EU) 2023/2844 VAN HET EUROPEES PARLEMENT EN DE RAAD van 13 december 2023 betreffende de digitalisering van de justitiële samenwerking en de toegang tot de rechter in grensoverschrijdende burgerlijke, handels- en strafzaken, en tot wijziging van bepaalde handelingen op het gebied van justitiële samenwerking

² Zie BNC-fiche: TK 28 januari 2022: 22112-3274

[2] De e-justice verordening heeft in zoverre impact op de nationale digitale autonomie, dat deze voorschrijft dat de grensoverschrijdende communicatie digitaal moet (tenzij voldaan is aan een nader omschreven uitzondering). Wel is het uitgangspunt bij deze digitalisering dat gebruik wordt gemaakt van de op de IT-infrastructuur e-CODEX gebaseerde decentrale ITsystemen, die interoperabiliteit moeten garanderen doordat elke Lidstaat desgewenst van eigen ITapplicaties gebruik kan maken. Hierdoor kan de nationale digitale autonomie worden geborgd. Als deze interoperabiliteit onvoldoende geborgd zou worden bij de implementatie van de e-Justiceverordening, zou dit de nationale digitale autonomie negatief kunnen beïnvloeden. Nederland heeft zich daarom tijdens de onderhandelingen over de e-Justice verordening hard gemaakt voor deze interoperabiliteit van Europese digitale systemen. Zo heeft Nederland bij de onderhandelingen over de e-Justice-verordening bereikt dat elementen van de gedecentraliseerde IT-systemen voor grensoverschrijdende communicatie, modulair worden opgezet, zodat lidstaten met hun bestaande nationale IT-systemen aan dit systeem kunnen aankoppelen. Momenteel worden de technische specificaties en voorwaarden voor de bouw van de IT-systemen nader uitgewerkt in door de Europese Commissie voorgezeten comitologie-onderhandelingen, die in Q1 van 2024 zijn gestart en in ieder geval doorlopen tot en met 2029. Tijdens deze dialoog zet Nederland zich in om te zorgen dat de gemaakte afspraken over interoperabiliteit en nationale IT-autonomie worden gevolgd.

Vraag (2):

Hoe wordt borging geregeld voor regio's met zwakke digitale infrastructuur?

Antwoord:

Nederland beschikt over een zeer hoogwaardige digitale infrastructuur, blijkt onder andere uit verschillende internationale vergelijkingen en uit de Staat van de Digitale Infrastructuur [1] die met de Kamer is gedeeld. Er is geen sprake van "regio's met zwakke digitale infrastructuur" zoals de vraag lijkt te suggereren. Een aandachtspunt is wel dat nog niet alle huishoudens in de buitengebieden kunnen beschikken over snel internet. Er wordt goede voortgang geboekt met de uitrol van glasvezel en bovendien zijn er steeds meer draadloze alternatieven waarmee deze huishoudens goed kunnen participeren in onze digitaliserende samenleving[2]. Dit antwoord is afkomstig van de Minister van Economische Zaken

[1] Kamerstuk 26643, nr. 1119

[2] Kamerstuk 26643, nr. 1224

Vraag (3):

Welke vitale knelpunten zijn gesignaleerd in landelijke regio's bij de

voorbereiding op de aankomende Cyberbeveiligingswet?

Antwoord:

Op verzoek van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft de Rijksinspectie Digitale Infrastructuur (hierna: RDI) een uitvoerings- en handhavingstoets (UHT) uitgevoerd op het concept van het Cyberbeveiligingsbesluit en de bijbehorende nota van toelichting. Mogelijke knelpunten die hieruit naar voren zijn gekomen, zijn meegenomen in bovengenoemd interdepartementaal implementatieproces.

Vraag (4):

Wat betekent de vertraagde implementatie van de NIS2- en CER-richtlijn voor kleine, essentiële entiteiten zoals agrarische coöperaties?

Antwoord:

Om organisaties op weg te helpen heeft de Rijksoverheid een zelfevaluatietool ontwikkeld waarmee organisatie een eerste beoordeling kunnen doen of ze als essentiële entiteit of belangrijke entiteit onder de Cyberbeveiligingswet komen te vallen.

In de periode tussen 17 oktober 2024 en de datum van inwerkingtreding van de Cyberbeveiligingswet gelden er voor organisaties, die onder die wet komen te vallen, geen verplichtingen vanuit de NIS2-richtlijn. Voor alle essentiële en belangrijke entiteiten gaan die verplichtingen pas gelden zodra de Cyberbeveiligingswet in werking treedt. Sommige andere bepalingen uit de NIS2-richtlijn hebben in genoemde overgangsperiode zogenoemde rechtstreekse werking. Dat betekent dat organisaties die van rechtswege onder de richtlijn vallen, in die periode bepaalde rechten zullen hebben, zoals het ontvangen van bijstand bij een cyberincident door een CSIRT.

Daarnaast wordt entiteiten aangeraden om zich alvast voor te bereiden op de komst van de Cyberbeveiligingswet.

Vraag (5):

Welke dekkingstekorten van C2000 (het communicatiesysteem voor hulpdiensten) in buitengebieden zijn aangepakt in 2024?

Antwoord:

Zoals ook beschreven in de Verzamelbrief Brandweer, Crisisbeheersing en Meldkamers van 6 februari jl. wordt er hard gewerkt aan de verbetering van de dekking van C2000 in gebieden met verminderde dekking (DIPP-gebieden). Hoewel gestreefd wordt naar het volledig optimaliseren van de radiodekking van C2000 is 100% dekking niet mogelijk. Het plaatsen van nieuwe opstelpunten heeft een doorlooptijd van twee tot drie jaar. Door het plaatsen van mobiele oplossingen, met een gemiddelde doorlooptijd van een tot anderhalf jaar, kunnen bestaande opstelpunten verbeterd worden. De totale lijst bestaat uit 95 DIPP-gebieden. Van de 95 gebieden zijn er momenteel 28 gebieden

opgelost, waarvan 12 gebieden in 2024. Het Ministerie van Justitie en Veiligheid doet vanuit operationeel oogpunt geen uitspraken over de locatie van individuele, bestaande of al opgeloste, DIPP-gebieden.

Vraag (6):

Zijn 'geofencing'-tests met NL-Alert uitgevoerd in landelijke regio's, en zo ja, wat waren de resultaten?

Antwoord:

Voor de implementatie van geofencing in NL-Alert zijn door de beheerder van NL-Alert (Landelijke Meldkamer Samenwerking) tests uitgevoerd met onder andere mobiele telefoon providers. Het doel van deze tests was om vast te stellen dat geofencing (op Iphone en Android-toestellen) op de netwerken van de mobiele telefonie providers en de broker van NL-Alert goed functioneert, en om waar nodig verbeteringen door te voeren. Dit heeft geleid tot het advies om begin september 2024 geofencing te implementeren in NL-Alert. Daarnaast is er een vervolgtraject ingericht voor de doorontwikkeling van geofencing om de uitzending van NL-Alert voor nog kleinere uitzendgebieden (vanaf 200 bij 200 meter) mogelijk te gaan maken. Dit traject loopt nog.

Vraag (7):

Kunt u, in hoeverre mogelijk, inzicht geven in de totale licentiekosten die over 2024 betaald zijn aan Microsoft?

Antwoord:

Het is niet mogelijk om inzicht te geven in de exacte omvang van de licentiekosten. Dit omdat de licentiekosten (naast overige kosten) deel uitmaken van de prijs die voor Microsoft producten wordt betaald. Wel kan desgewenst inzage worden geboden in de uitgaven aan Microsoft producten.

Vraag (8):

Zijn de licentiekosten van grote techleveranciers waar de overheid in grote mate afhankelijk van zijn verhoogd over 2024? Hoeveel meer betaalt u aan de licenties ten opzichte van eerdere jaren?

Antwoord:

Over 2024 zijn er geen uitzonderlijke verhogingen waar te nemen. Vanuit rijksbreed categoriemanagement en strategische leveranciersmanagement wordt voortdurend gewerkt aan een gezonde samenwerking met IT-leveranciers. Eventuele verhoging van licentiekosten zijn onderwerp van gesprek. In het geval van voorgestelde aanpassingen in samenwerkingsvoorwaarden (zoals duurdere licenties) wordt via meerdere instrumenten gewerkt aan alternatieve oplossingen; dit kan juridisch van aard zijn, of via andere (open source) technische oplossingen.

**Overkoepelende / overige vragen die betrekking hebben op
bovenstaande slotwetten**

De beantwoording van de overkoepelende vragen wordt verzorgd door de
minister van Binnenlandse Zaken en Koninkrijksrelaties.