36 600 VI Vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2025

Nr. 15 VERSLAG HOUDENDE EEN LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 7 november 2024

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.

De vragen zijn op 7 oktober 2024 voorgelegd aan de minister van Justitie en Veiligheid. Bij brief van 5 november 2024 zijn ze door de minister 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,
Palmen

Adjunct-griffier van de commissie,
Muller

Vragen en antwoorden

42

Bent u voornemens om bij de Voorjaarsnota extra geld vrij te maken voor de Autoriteit Persoonsgegevens (AP) voor het uitvoeren van haar taken indien de AP aangeeft dat dat noodzakelijk is?

Antwoord

De Autoriteit Persoonsgegevens (AP) vervult een belangrijke rol als onafhankelijke toezichthouder in de gegevensbeschermingsketen. Het kabinet Rutte IV heeft daarom extra middelen uitgetrokken om de capaciteit van de AP uit te breiden. Het budget van de AP voor het toezicht op de Algemene Verordening Gegevensbescherming (AVG) groeit hierdoor naar ruim 45 miljoen euro structureel vanaf 2025. De AP ontvangt daarnaast bijdragen van de ministeries van Financiën, Economische Zaken en Binnenlandse Zaken Koninkrijksrelaties voor andere toezichtstaken. Dat brengt het totale budget van de AP voor volgend jaar op circa 49 miljoen euro. Dat is ongeveer een verdubbeling van het budget binnen vijf jaar. De AP is een onafhankelijke toezichthouder en bepaalt zelf waar zij haar financiële middelen aan uitgeeft en waar zij prioriteiten legt. Het toekennen van meer middelen aan de AP ziet het kabinet op dit moment niet als het middel bij uitstek om een goede omgang met persoonsgegevens verder te borgen.

43

Bereiden het departement en de uitvoeringsorganisaties zich voor op NIS2? Zo ja, hoe?

Antwoord

De voorbereidingen van de implementatie van de NIS2-richtlijn gaan langs diverse lijnen. De NIS2-richtlijn wordt geïmplementeerd in de Cyberbeveilingswet. Er zijn door de vakdepartementen en daartoe behorende uitvoeringsorganisaties uitvoeringstoetsen en/of handhaafbaarheidtoetsen gedaan en er wordt hard gewerkt om daar uitwerking aan te geven. De beoogde toezichthouders en CSIRTs hebben middelen gekregen om hun capaciteit uit te breiden en technische en organisatorische aanpassingen door te voeren.

Daarnaast zijn er vanuit de Rijksoverheid voor de verschillende sectoren én uitvoeringsorganisaties, tools en kennis-en adviesproducten ontwikkeld die organisaties kunnen gebruiken of inzetten om zich beter voor te breiden op de komende inwerkingtreding van de Cyberbeveiligingswet. Zo heeft de Rijksinspectie Digitale Infrastructuur (RDI) bijvoorbeeld een vragenlijst ontwikkeld, waarmee organisaties zelf een eerste beoordeling kunnen doen of ze onder de NIS2-richtlijn vallen en of ze in dat verband aangemerkt worden als essentiële entiteit of belangrijke entiteit. Ook is vanuit de Rijksoverheid een NIS2-Quickscan gelanceerd: een hulpmiddel voor organisaties die willen weten hoe zij zich kunnen voorbereiden op de komende implementatie van de NIS2-richtlijn. Tevens hebben het NCSC en DTC diverse kennis- en adviesproducten ontwikkeld die organisaties kunnen helpen om te voldoen aan de aankomende regelgeving.

Verder worden organisaties door betrokken ministeries en uitvoeringsorganisaties voortdurend actief benaderd en gewezen op de maatregelen die ze nu al kunnen treffen. Dit wordt gecoördineerd uitgevoerd. Wel is ieder vakdepartement en uitvoeringsorganisatie primair verantwoordelijk voor het informeren en activeren van hun eigen sector en achterban.

De Rijksoverheid raadt organisaties dan ook aan deze maatregelen te nemen om de continuïteit van de bedrijfsprocessen (beter) te waarborgen. Voor organisaties die straks moeten voldoen aan de komende wetgeving is het dan ook van belang vroegtijdig te beginnen met de voorbereidingen. De risico’s die organisaties en systemen lopen, zijn er immers nu ook al.

Ook is een publiek-privaat NIS2-overleg actief met vertegenwoordigers uit de Rijksoverheid en diverse brancheorganisaties.

44

Is het budget van de politie toereikend om te handhaven op online kindermisbruik? Investeert u de komende jaren in het uitbreiden en uitrusten van het Team Bestrijding Kinderpornografie en Kindersekstoerisme (TBKK)? Zo ja, wat is de gewenste extra capaciteit van het TBKK? Zo niet, hoe verenigt u dit met het groeiende aantal meldingen van online kindermisbruik?

Antwoord

Online seksueel kindermisbruik is een zeer ernstig strafbaar feit met langdurige ernstig ontwrichtende gevolgen voor een slachtoffer en diens omgeving. De aanpak van online seksueel kindermisbruik bij de politie wordt uitgevoerd door de Teams ter Bestrijding van Kinderpornografie en Kindersekstoerisme (TBKK´s). Met de motie Hermans c.s. [1] zijn middelen ter beschikking gesteld om de aanpak van seksuele misdrijven en online kinderpornografisch materiaal een impuls te geven. Hiervan ontvangt de politie vanaf 2024, in oplopende tranches, structureel 4 miljoen euro om te investeren in de versterking van de werkwijze en digitale mogelijkheden van de TBKK ter aanwending van de bestrijding van digitale zedendelicten. Als gevolg van deze investering is de formatie van de TBKK met 24 fte uitgebreid naar een totaal van 175 fte. De bezetting van de TBKK is sinds eind 2022 met 25 fte gestegen naar een totaal van 153 fte eind april 2024.

Gezien de massale aard van online seksueel kindermisbruik, in combinatie met de schaarse politiecapaciteit, is het echter nodig om naast de reguliere opsporing en vervolging ook in te zetten op alternatieve interventies of verstoringsacties, zoals de vorig jaar uitgevoerde actieweek van de politie waar stopgesprekken werden gevoerd met verdachten van het downloaden van beeldmateriaal van online seksueel kindermisbruik, gerichte acties op het darkweb of het ontoegankelijk maken van fora waar beeldmateriaal gedownload kan worden. Maar ook preventieve hulpverlening zoals die wordt aangeboden bij Stop it Now, onderdeel van stichting Offlimits, speelt een rol in de aanpak van dit fenomeen. Verder wordt er nog ingezet op nieuwe en effectievere EU-regelgeving ter voorkoming en bestrijding van seksueel misbruik van kinderen. Onder andere door middel van de EU-Verordening ter bestrijding van online seksueel kindermisbruik. Het doel van deze verordening is om de verspreiding van beelden van online seksueel kindermisbruik tegen te gaan. Het ontwerp stelt regels om ervoor te zorgen dat de verschillende aanbieders van tussenhandeldiensten meer verantwoordelijkheid nemen om de eigen diensten schoon te maken en houden van online materiaal van seksueel kindermisbruik. Voorbeelden van dergelijke diensten zijn hostingdiensten, online platforms en interpersoonlijke communicatiediensten.

In het regeerprogramma is opgenomen dat de aanpak van seksueel kindermisbruik wordt geïntensiveerd. Daarom is het onverminderd

[1] *Kamerstukken II* 2021/22, 35925, nr. 13.

voortzetten van de aanpak een prioriteit voor dit kabinet en wordt bezien of er extra stappen gezet kunnen worden

45

Hoeveel budget heeft de politie voor ICT?

Antwoord

In de begroting van de politie is voor 2025 668 miljoen euro opgenomen voor informatievoorziening.

46

Welke nieuwe taken volgen er uit digitale EU-regelgeving voor de AP? Kunt u per verordening of wet toelichten welke middelen de AP hiervoor ontvangt? Kunt u hierbij aangeven er sprake is van cofinanciering uit verschillende departementen (zoals bij het ministerie van EZ voor toezicht op de DGA) en welk departement daar verantwoordelijk voor is?

Antwoord

De AP houdt zich bezig met verschillende taken rondom digitale EU-wetgeving. Om deze taken uit te kunnen voeren ontvangt de AP middelen vanuit verschillende ministeries. Welk ministerie dat is, is afhankelijk van de desbetreffende EU-wetgeving. Deze geldstromen lopen via de begroting van het ministerie van Justitie en Veiligheid.

Ter verduidelijking:

Wetgeving	**Taken**	**Middelen**	**Ministerie**
DSA	Taken die voorvloeien uit DSA: • Artikel 26 lid 3 en 28 lid 2 en 3 DSA: deze houden verband met het profileren van gegevens van kinderen/bijzondere persoonsgegevens met als doel adverteren (AP	2024: € 355.000 2025: € 516.000	EZ EZ

	is hier aangewezen als toezichthouder). - Artikel 40 lid 8 onder d: adviesrol richting ACM over de toelating van erkende onderzoekers.		
DGA	Taken die voortvloeien uit DGA: - Adviesrol richting ACM bij de aanvraag voor registratie van databemidddelingsdiensten. - Adviesrol richting ACM bij de aanvraag voor registratie van data-altruïstische organisaties.	€ 121.000 van BZK (structureel) € 120.000 van EZ (structureel)	EZ (50%) en BZK (50%)
Dataverordening	Voorbereiding op taken die voortkomen uit: - De overlap tussen AVG en DV. - Artikelen 4 en 5 DV (bepaling AVG-grondslag). - Hoofdstuk 5 van de DV (in voorlopige uDV aangewezen als toezichthouder).	Incidenteel voor voorbereiding: 2024: € 680.000 toegekend (€ 170.000 van EZ en € 510.000 van BZK) 2025: Het deel voor 2025 van EZ is nog niet toegekend (€ 255.000). Bijdrage van BZK is wel toegekend (€ 765.000)	EZ (25%) en BZK (75%)

		Op de gevraagde structurele middelen uit de Uitvoeringstoets is nog niet gereageerd.	
AI-verordening	Voorbereidend werk toezicht AI-verordening	Voor 2024: €1.084.000 Voor 2025: Nader te bepalen	EZ

47

Welke middelen worden er vrijgemaakt voor de AP voor het uitvoeren van de aanbevelingen uit het rapport 'Ongekend Onrecht'?

Antwoord

De Autoriteit Persoonsgegevens krijgt vanaf 2023 tot 2033 ongeveer 2,6 miljoen euro aan Parlementaire ondervragingscommissie kinderopvangtoeslagen (POK)/ Werk aan Uitvoering (WaU)-middelen. Hiermee versterkt de AP het toezicht op het gebruik van algoritmes, voorkomt negatieve gevolgen van het gebruik van algoritmes waarin persoonsgegevens worden gebruikt en signaleert en pakt de risico’s hieromtrent aan.

48

Waarom kent de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) een stabiele jaarlijkse financiering, in plaats van een financiering die meegroeit met het groeiende aantal meldingen waarop zij moet handhaven? Heeft u de mogelijkheid om incidenteel geld vrij te maken als de ATKM dit nodig heeft voor haar taken?

Antwoord

Voor de inrichting van de autoriteit is in de voorbereidingsfase voor zowel de aanpak van kinderpornografisch materiaal als voor de aanpak

van terroristische online inhoud een inschatting gemaakt van de personele en financiële consequenties. Voor de aanpak van kinderpornografisch materiaal is een business case opgesteld en voor de implementatie van de verordening online terroristisch online materiaal is een verkenning uitgevoerd. De resultaten van beide zijn input geweest voor het toekennen van financiering aan de autoriteit en voor het opstellen van een organisatie– en formatierapport. Hierin staan de kaders voor de omvang en inrichting van de organisatie beschreven.

Voor de ATKM is vanuit de begroting van het ministerie van J&V een budget beschikbaar gesteld van ca. € 5,2 miljoen in 2023 oplopend tot ca. € 6,4 miljoen euro structureel vanaf 2025. De ATKM kan de komende periode groeien naar maximaal 34 fte, waaronder 3 bestuurders.

De noodzakelijke omvang van de ATKM is niet alleen afhankelijk van het aantal meldingen dat zij ontvangt, maar kan ook beïnvloed worden door het eigen onderzoek dat zij naar meldingen kan doen op basis van de wettelijke taak. Ook hier kunnen verwijderbevelen uit voortvloeien. Eventuele additionele financiering is op dit moment niet aan de orde. In de reguliere begrotingsprocessen en in de evaluaties van beide wetten kan de financiering aan de orde komen indien daar aanleiding voor is.

49

Hoeveel van de 46 miljoen euro voor het Nationaal Cybersecurity Center (NCSC) gaat naar preventie van cyberrisico’s en hoeveel gaat naar de aanpak en het herstel van cyberrisico’s?

Antwoord

Het NCSC heeft tot taak om verschillende organisaties zowel preventief in geval van dreigingen, de koude fase, als in situaties wanneer er een incident is, de warme fase, te informeren, adviseren of bijstand te verlenen. Als gevolg daarvan zijn veel producten en diensten van het NCSC waardevol in zowel de koude als de warme fase. Daarbij is het vrijwel onmogelijk om onderscheid tussen genoemde activiteiten te maken als het gaat om de inzet van middelen. Een voorbeeld van een product dat in beide fase zeer relevant is, is het in bovenbedoeld verband informeren van mogelijke slachtoffers en doelwitten van een cyberdreiging of -incident. Hiermee worden zowel organisaties geïnformeerd die slachtoffer zijn van een incident en met deze informatie verdere schade kunnen beperken, en organisaties die doelwit zijn en

daarmee maatregelen kunnen nemen om te voorkomen dat zij daadwerkelijk slachtoffer worden.

50

Welk percentage van de begroting van uitvoeringsorganisaties van het ministerie van Justitie en Veiligheid (JenV) is beschikbaar voor cybersecurity? Is er ook een internationale benchmark?

Antwoord

Binnen de rijksbegroting worden de middelen die beschikbaar zijn voor cybersecurity niet apart begroot. Hierdoor kan ik niet aangeven welk percentage van de begroting beschikbaar is voor cybersecurity. Op dit moment ben ik niet op de hoogte van internationale benchmarks die een begrip als cybersecurity kunnen definiëren en vervolgens representatief benchmarken over verschillende organisaties.

51

Aan het budget apparaat wordt in 2025 6,2 miljoen euro, in 2026 11 miljoen euro, aflopend naar 3,6 miljoen euro vanaf 2029, toegevoegd om aan maatregelen vanuit de EU te voldoen waarmee de regelgeving binnen de EU op het gebied van digitalisering wordt geüniformeerd en verbeterd. Kunt u nader toelichten om welke verordeningen het hier gaat?

Antwoord

Het betreft hier de Artificiële Intelligentie (AI) Verordening, de Network and Information Security 2 (NIS2)-richtlijn en e-Justice.

52

Welke sectorale toezichthouders zijn betrokken bij het implementeren van en toezien op de NIS2-richtlijn? Welke middelen krijgt ieder van hen voor deze nieuwe taken? In het geval dat deze middelen bestaan uit cofinanciering uit verschillende departementen: wie is de coördinator van dit budget?

Antwoord

De vakdepartementen gaan zelf over hun eigen sectoren en de departementale begrotingen. Zij hebben alle de kosten in relatie tot de implementatie van de richtlijn geraamd en deze verwerkt in de departementale begrotingen. Indien er sprake is van cofinanciering, dan

zal dit via het normale begrotingsproces worden verwerkt, en vindt er sturing plaats conform de sturingsmodellen van de betreffende departementen. Het toezicht zal in hoofdzaak bestaan uit het toezien op de naleving van de meldplicht, zorgplicht en registratieplicht alsook de handhaving daarvan. De toezichthouders zullen onderling werkafspraken maken om ervoor te zorgen dat zij doeltreffend en doelmatig uitvoering geven aan hun taken. Dit is een gebruikelijke werkwijze.

Ik verwacht dat het voorstel voor de Cyberbeveiligingswet in het vierde kwartaal van 2024 voor advies worden aangeboden aan de Afdeling advisering van de Raad van State. Afhankelijk van de tijd die nodig is voor het advies en de verwerking daarvan, zal het voorstel naar verwachting in het eerste kwartaal van 2025 naar uw Kamer worden gestuurd.

53

Hoe heeft u het budget voor het implementeren van de NIS2-richtlijn ingeschat? Kunt u met zekerheid zeggen dat dit budget toereikend is? Zo niet, uit welk budget worden tegenvallers gefinancierd?

Antwoord

De verantwoordelijke departementen hebben alle de kosten in relatie tot de implementatie van de richtlijn geraamd en deze verwerkt in de departementale begrotingen. Dit loopt op tot circa € 80 miljoen structureel in 2029 dit is inclusief de budgettaire gevolgen van de inwerkingtreding van de Wet weerbaarheid kritieke entiteiten. Naar gelang de implementatie van het wetsvoorstel vordert kunnen waar nodig bijstellingen van deze ramingen worden doorgevoerd, bijvoorbeeld naar aanleiding van de consultatie op de amvb die op grond van de Cyberbeveiligingswet wordt voorbereid.

54

Kunt u uitleggen waarom de subsidie voor Offlimits afneemt, terwijl de hoeveelheid meldingen die zij ontvangt onverminderd toeneemt? Waarom is er niet gekozen voor een hogere bijdrage van het Rijk of een financieringsmodel op basis van bereikbaarheid?

Antwoord

De subsidie die door het ministerie van Justitie en Veiligheid aan Offlimits wordt verstrekt is sinds 2022 flink verhoogd (van € 627.000

naar € 2,5 miljoen), waarmee erkend is dat Offlimits een onmisbare rol vervult met betrekking tot het tegengaan van illegale content, in het bijzonder online seksueel misbruik van kinderen en illegale inhoud.

In het hoofdlijnenakkoord is besloten tot een Rijksbrede taakstelling op de subsidies oplopend tot in totaal € 1 miljard. Daarvan geldt een taakstelling van € 29 miljoen voor het ministerie van Justitie en Veiligheid. De taakstelling is op basis van de budgetten in de begroting evenredig verwerkt per organisatie, wat heeft geleid tot een langzaam dalende subsidieraming. Over de uiteindelijke daadwerkelijke verdeling per organisatie dient nog interne besluitvorming plaats te vinden.

55

Wordt Offlimits mede gefinancierd door het ministerie van BZK vanuit het beleidsdoel Online Kinderrechten vanwege haar preventieve taken? Zo ja, welk departement coördineert de financiering richting de organisatie? Zo niet, kent de financiering vanuit het ministerie van JenV bepaalde oormerken of voorwaarden waaronder het wordt toegekend?

Antwoord

Nee, Offlimits ontvangt vanuit de Rijksoverheid op dit moment enkel subsidie van het ministerie van Justitie en Veiligheid. Voor elke subsidieverstrekking geldt dat deze verbonden is aan bepaalde voorwaarden. Daartoe worden jaarlijks afspraken gemaakt in het subsidiebesluit. Voor 2024 ziet dat bijvoorbeeld op bepaalde stappen die Offlimits dient te nemen op het vlak van IT, zoals aansluiten bij de BIO: Baseline Informatiebeveiliging Overheid.