Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

420

Vragen van het lid **Kathmann** (GroenLinks-PvdA) aan de Staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Volksgezondheid, Welzijn en Sport over *het afhandelen van de hack op Clinical Diagnostics en de gevolgen voor gedupeerden* (ingezonden 10 oktober 2025).

Antwoord van Staatssecretaris **Tielen** (Volksgezondheid, Welzijn en Sport), mede namens de Minister van Volksgezondheid, Welzijn en Sport (ontvangen 18 november 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 299.

Vraag 1
Wat zijn de meest recente ontwikkelingen rondom het datalek bij het bevolkingsonderzoek naar baarmoederhalskanker?

Antwoord 1
In de Kamerbrief van 1 september 2025[1] kondigde ik aan dat Bevolkingsonderzoek Nederland (BVO NL) een brief zou sturen naar alle betrokkenen die hebben deelgenomen aan het bevolkingsonderzoek baarmoederhalskanker en van wie de gegevens naar het laboratorium Clinical Diagnostics zijn gestuurd. De brieven zijn halverwege september verstuurd. Het klantcontactcentrum van BVO NL was opgeschaald en uitgebreid met een speciale informatielijn met specialisten op het gebied van crisistelefonie. Dit zodat alle vragen die naar aanleiding van de brieven zijn gesteld snel beantwoord konden worden. Er is op dit moment met de reguliere bezetting voldoende capaciteit om de vragen aan te kunnen en op tijd te beantwoorden.
De toezegging om uw Kamer blijvend op de hoogte te houden van de laatste ontwikkelingen staat nog steeds.

Vraag 2
Wat is de stand van zaken omtrent de maatregelen die u aankondigde in uw brief van 1 september 2025?[2] Kunt u dit per maatregel toelichten?

Antwoord 2
Hieronder geef ik per maatregel uit de brief van 1 september 2025 een toelichting op de stand van zaken.

[1] Kamerstukken II, 2024/25, 32 761, nr. 330.
[2] Kamerstuk 32 761, nr. 330.

ah-tk-20252026-420
ISSN 0921 - 7398
's-Gravenhage 2025

De samenwerking met het betreffende laboratorium is door BVO NL tot nader order opgeschort. Twee laboratoria die betrokken zijn bij het bevolkingsonderzoek baarmoederhalskanker hebben het werk van het getroffen laboratorium overgenomen. Bij deze laboratoria worden door Z-CERT vanaf heden permanente kwetsbaarhedenchecks uitgevoerd op de systemen van deze laboratoria die zijn ontsloten aan het internet.

Z-CERT heeft op verzoek van de Minister van VWS alle laboratoria benaderd die zijn betrokken bij de bevolkingsonderzoeken naar kanker en screeningsprogramma's rond zwangerschap en geboorte. Het doel is om die ook toe te voegen aan de scanningsdienst van Z-CERT. Hierover is uw Kamer geïnformeerd op 30 september 2025.[3] Inmiddels zijn nagenoeg alle benaderde laboratoria toegevoegd aan de scanningsdienst. Met deze dienst van Z-CERT wordt continu gemonitord op bekende kwetsbaarheden op de systemen van deze laboratoria die benaderbaar zijn via het internet. De resultaten worden aan de laboratoria teruggekoppeld, zodat zij waar nodig maatregelen kunnen treffen.
BVO NL heeft zelf ook een quickscan uit laten voeren naar acute risico's bij de twee laboratoria die momenteel werkzaamheden uitvoeren voor het bevolkingsonderzoek baarmoederhalskanker. Hieruit kwam naar voren dat deze laboratoria voldoende veilig zijn.

BVO NL heeft in afstemming met het RIVM een onderzoek ingesteld naar de exacte omvang en de oorzaak van deze hack.

De oorzaak van de hack vormt onderwerp van nader onderzoek. Op dit moment is nog niet concreet te duiden wanneer de uitkomsten daarvan bekend zullen worden.

Er is onderzoek gestart naar wat BVO NL kan verbeteren aan onder meer dataminimalisatie, aanbestedingseisen en bewaartermijnen.

Afronding van dit onderzoek wordt eind dit jaar verwacht.

BVO NL heeft melding gedaan bij de Autoriteit Persoonsgegevens (AP) en de Inspectie Gezondheidszorg en Jeugd (IGJ). De AP en de IGJ zijn inmiddels beide een onderzoek gestart.

De AP en de IGJ voeren hun toezichthoudende taak onafhankelijk uit. Zij bepalen daarbij hun eigen werkwijze en planning voor de onderzoeken. Op dit moment beschik ik niet over nadere informatie over deze onderzoeken.

Het Openbaar Ministerie en de politie hebben bekend gemaakt strafrechtelijk onderzoek te doen naar het datalek.

Het is niet aan mij hier nader op in te gaan, hiervoor verwijs ik naar het Openbaar Ministerie.

Het RIVM heeft contact gelegd met het Nationaal Cyber Security Centrum (NCSC) met het verzoek om assistentie. Het NCSC heeft de coördinatie van dit cyberincident inmiddels overgedragen aan Z-CERT.

Zoals gezegd, monitort Z-CERT momenteel de twee laboratoria die werkzaamheden uitvoeren voor het bevolkingsonderzoek baarmoederhalskanker.
Z-CERT heeft op verzoek van de Minister van VWS daarnaast alle laboratoria benaderd die zijn betrokken bij de bevolkingsonderzoeken naar kanker en screeningsprogramma's rond zwangerschap en geboorte. Dit met als doel om die ook toe te voegen aan de scanningsdienst van Z-CERT. Inmiddels zijn nagenoeg alle benaderde laboratoria toegevoegd aan de scanningsdienst. De resultaten worden aan de laboratoria teruggekoppeld.

Tot slot brengt het ministerie van VWS databeveiliging permanent onder de aandacht in (bestuurlijke) gesprekken met partners uit het veld.

Dit betreft doorlopende inzet. De Minister van VWS geeft hier bijvoorbeeld invulling aan door zorgbestuurders per brief op te roepen om prioriteit te

[3] Kamerstukken II, 2024/25, 32 761, nr. 333.

geven aan het nemen van de nodige maatregelen, te beginnen met het voldoen aan de norm, de NEN 7510.

Vraag 3
Zijn inmiddels alle gedupeerden op de hoogte dat zij getroffen zijn door het datalek en is voor hen duidelijk welke data van hen is buitgemaakt?

Antwoord 3
In september zijn alle betrokkenen die hebben deelgenomen aan het bevolkingsonderzoek baarmoederhalskanker en van wie gegevens met het laboratorium zijn gedeeld, geïnformeerd. In de brieven heeft BVO NL ook aangegeven welke persoonsgegevens BVO NL met het laboratorium heeft gedeeld. Er is op dit moment niet te zeggen welke gegevens bij de hack zijn bemachtigd.

Vraag 4
Heeft u gemerkt dat het datalek heeft geleid tot een lagere bereidheid om mee te doen aan volgende bevolkingsonderzoeken? Wat doet u om de deelname op peil te houden?

Antwoord 4
De deelname aan het bevolkingsonderzoek baarmoederhalskanker wordt nauwlettend in de gaten gehouden. Normaal gesproken is er een dip in de deelname in de zomervakantie en gaat de deelname daarna weer omhoog. In de eerste weken na de zomer bleef de instroom van ingestuurde testen bij de labs achter, maar dit lijkt de afgelopen periode weer wat bijgetrokken. Om te kunnen constateren of dit ook daadwerkelijk de deelname heeft beïnvloed, moet over een langere periode gekeken worden. Ter illustratie: het is bijvoorbeeld mogelijk dat vrouwen de zelfafnameset iets langer laten liggen vanwege de datahack, maar op een later moment toch nog deelnemen. Zodra we hier meer over kunnen zeggen en als sprake is van een significante verandering in de deelname, zal ik uw Kamer daarover informeren.

Vraag 5
Is gebleken dat gedupeerden van het datalek vaker het doelwit zijn van phishing, fraude en andere online criminaliteit? Heeft u cijfers of analyses waaruit dit blijkt?

Antwoord 5
Dat kan ik niet aangeven, omdat in geval van phishing, fraude of andere online criminaliteit het de vraag is of daarbij gebruik is gemaakt van persoonsgegevens die betrokken zijn geweest bij de datahack, of dat de gebruikte persoonsgegevens op andere wijze in handen zijn gekomen van criminelen.

Vraag 6
Hoe lang blijft het klantcontactcentrum van Bevolkingsonderzoek Nederland bereikbaar voor gedupeerden? Zorgt u ervoor dat gedupeerden altijd ergens terecht kunnen met zorgen en vragen?

Antwoord 6
Het klantcontactcentrum van BVO NL is tijdens kantooruren altijd bereikbaar. Hier kunnen mensen terecht voor vragen in relatie tot de bevolkingsonderzoeken, waaronder uiteraard ook met vragen over de datahack. Het klantcontactcentrum van BVO NL was opgeschaald, zodat de grote hoeveelheid vragen die kwam naar aanleiding van de datahack snel beantwoord werd. Die opschaling is inmiddels weer afgebouwd, maar het klantcontactcentrum blijft beschikbaar voor alle vragen en is op dit moment in staat om alle vragen op tijd te beantwoorden.

Vraag 7
Heeft u op basis van uw contact met gedupeerden, of op basis van hun klachten en signalen, aanvullende acties ondernomen om tegemoet te komen aan hun behoeften?

Antwoord 7
Naar aanleiding van de eerste brieven die BVO NL had verzonden in de week van 18 augustus, zijn veel reacties gekomen. Er was kritiek op de inhoud van de brief en BVO NL kreeg vele suggesties ter verbetering, onder andere van de Nationale ombudsman. Deze suggesties zijn door BVO NL meegenomen bij het opstellen van de tweede ronde brieven die naar ruim 941.000 mensen zijn verzonden. Ik heb destijds de brief van de Ombudsman direct doorgestuurd naar BVO NL met het verzoek deze mee te nemen in de formulering van die tweede ronde brieven. Ook andere signalen en suggesties zijn meegenomen bij het opstellen van de tweede ronde brieven.

Vraag 8
Bent u bekend met maatschappelijke initiatieven, zoals de Digitale Dolle Mina's, die gedupeerden samenbrengen en informatie verschaffen?[4] Hoe trekt u samen met deze initiatieven op om gedupeerden te bereiken?

Antwoord 8
Ik ben bekend met deze initiatieven. De primaire informatievoorziening verloopt via BVO NL. Deelnemers van het bevolkingsonderzoek baarmoederhalskanker die zijn getroffen door de datahack, zijn hierover geïnformeerd door BVO NL. Naast de persoonlijke brieven, zijn er de breed gedeelde nieuwsberichten geweest op onder andere 11 augustus en 29 augustus jl. om mensen te informeren over de datahack.

Vraag 9
Is inmiddels duidelijk geworden hoe de hack en het datalek plaats hebben kunnen vinden? Zo ja, welke oorzaak lag daaraan ten grondslag en hoe gaat dit in de toekomst worden voorkomen? Zo nee, wanneer kan de Kamer de uitkomst van dat onderzoek verwachten?

Antwoord 9
De oorzaak van de hack vormt onderwerp van nader onderzoek. Op dit moment is nog niet concreet te duiden wanneer de uitkomsten daarvan bekend zullen worden. Uiteraard zal op basis van de uitkomsten worden bezien welke lessen daaruit kunnen worden getrokken.

Vraag 10
Voert de Inspectie Gezondheidszorg en Jeugd (IGJ) vooraf checks uit naar de informatieveiligheid van partnerorganisaties bij nieuwe samenwerkingen, zoals laboratoria? Zo ja, wat zijn de aandachtspunten van de IGJ bij die checks? Zo nee, waarom wordt dat niet gedaan?

Antwoord 10
Nee, de IGJ voert hier niet vooraf checks op uit. Er is geen verplichting om samenwerkingen zoals hier omschreven (vooraf) bij de IGJ te melden.
De norm voor informatiebeveiliging (NEN 7510) stelt dat organisaties zelf de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig moeten monitoren, beoordelen en evalueren. De IGJ houdt achteraf toezicht op het voldoen aan de eisen voor informatiebeveiliging.

Vraag 11
Zijn er aanvullende beveiligingsmaatregelen die dit kabinet gaat invoeren om de tijd totdat de behandeling van de Cyberbeveiligingswet is afgerond te overbruggen? Zo ja, welke maatregelen zijn dat? Zo nee, hoe gaat u ervoor zorgen dat het risico op datalekken zoals deze zo klein mogelijk wordt?

Antwoord 11
Zorgaanbieders zijn in de eerste plaats zelf wettelijk verantwoordelijk voor hun informatiebeveiliging. Zij bepalen welke maatregelen genomen moeten worden om de risico's op het gebied van informatiebeveiliging te beheersen. Als stelselverantwoordelijke neemt de Minister van VWS de regie om het zorgveld hierbij te ondersteunen. Dit doet hij door zich in het huidige beleid

[4] www.digitaledollemina.nl

te richten op het stimuleren van bewustwording, passende hulp te bieden, toezicht te versterken en te ondersteunen bij incidenten.

Vraag 12
Hebben de politie en het Openbaar Ministerie vooruitgang kunnen boeken in het vinden van de datasets op het *dark web* en ook in het vinden van de daders? Heeft Z-CERT bij het monitoren van de data al gezien dat het op het *dark web* is verschenen?

Antwoord 12
Het Openbaar Ministerie heeft bekend gemaakt strafrechtelijk onderzoek te doen naar het datalek. Het is niet aan mij om hier nader op in te gaan, hiervoor verwijs ik naar het Openbaar Ministerie.
Wat betreft Z-CERT, ben ik hier in de beantwoording van de Kamervragen van het lid Kathmann van 9 september 2025 op ingegaan.[5] In het algemeen kan ik over de monitoring van Z-CERT alleen aangeven dat de resultaten van de monitoring aan de laboratoria worden teruggekoppeld zodat zij waar nodig maatregelen kunnen treffen.

Vraag 13
Heeft u collega-bewindspersonen op de hoogte gesteld van deze casus en van het belang van gegevensbeveiliging om dergelijke incidenten buiten de zorg ook te voorkomen? Zo nee, waarom niet? Zo ja, heeft het kabinet een plan gemaakt om bij alle departementen en hun ketenpartners het risico op datalekken te verminderen?

Antwoord 13
Mijn collega-bewindspersonen zijn op de hoogte gesteld van en bijgepraat over de datahack, onder andere op vrijdag 8 augustus, vrijdag 15 augustus en vrijdag 29 augustus 2025. Cybersecurity en digitale weerbaarheid zijn permanent onderwerp van aandacht binnen de hele overheid.

Vraag 14
Kunt u aangeven wanneer verdere informatie en uitkomsten van lopende onderzoeken naar de Kamer worden gestuurd en met betrokkenen worden gedeeld?

Antwoord 14
Zoals in de beantwoording hiervoor is aangegeven, verwacht ik van sommige onderzoeken de uitkomsten in het najaar. Van andere onderzoeken kan ik op dit moment nog niet concreet duiden wanneer de uitkomsten daarvan bekend worden. Uiteraard zal ik uw Kamer nader informeren zodra dat mogelijk is.

Vraag 15
Kunt u deze vragen afzonderlijk beantwoorden en, indien van toepassing, betrekken bij de eerstvolgende periodieke update aan de Kamer over het datalek?

Antwoord 15
Dat zal ik doen.

[5] Aanhangsel Handelingen II 2024/2025, nr. 3049.