Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

3049

Vragen van het lid **Kathmann** (GroenLinks-PvdA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister en Staatssecretaris van Volksgezond, Welzijn en Sport over *de hack op een lab van Bevolkingsonderzoek Nederland:* (ingezonden 27 augustus 2025).

Antwoord van Staatssecretaris **Tielen** (Volksgezondheid, Welzijn en Sport), mede namens de Minister van Volksgezondheid, Welzijn en Sport (ontvangen 9 september 2025).

Vraag 1
Wat is de stand van zaken omtrent de maatregelen die u aankondigt in uw recente Kamerbrief over het datalek bij het bevolkingsonderzoek naar baarmoederhalskanker?[1] Zijn alle gedupeerden van de hack inmiddels op de hoogte dat hun gegevens zijn gelekt?

Antwoord 1
Ik betreur het dat zoveel mensen in Nederland getroffen zijn door deze hack. Extra erg is het dat niet bekend is of alles nu bekend is. Zo hebben we, zoals ik in mijn brief van 1 september 2025 aan uw Kamer heb laten weten, wij tot onze spijt moeten constateren dat er nog meer deelnemers dan in eerste instantie gedacht, door de hack getroffen zijn.[2] Dit gaat om circa 230.000 mensen extra en het is niet uit te sluiten dat het hierbij blijft. In reactie op dit nieuws heeft Bevolkingsonderzoek Nederland (BVO NL) besloten om alle deelnemers van wie gegevens met het betreffende laboratorium zijn gedeeld, te informeren. Dat gaat om 941.000 deelnemers die naar verwachting half september worden geïnformeerd. Onder hen zitten ook de 485.000 mensen van wie al eerder bekend was dat zij waren getroffen door deze hack, en waarvan de meesten in de week van 18 augustus hierover een brief van BVO NL hebben ontvangen. Deze groep ontvangt dus opnieuw een brief. De tweede brief bevat informatie over welke gegevens door BVO NL zijn gedeeld met het laboratorium, hoe misbruik herkend en voorkomen kan worden en waarom BVO NL bepaalde gegevens gebruikt.
In de brief aan uw Kamer van 11 augustus 2025 zijn verschillende maatregelen aangekondigd met als doel de impact van de hack te beperken.[3] In de

[1] Kamerstuk 32 761, nr. 327.
[2] Kamerstuk II, 2024/25, 2025Z15722
[3] Kamerstuk II, 2024/25, 32 761, nr. 327

ah-tk-20242025-3049
ISSN 0921 - 7398
's-Gravenhage 2025

brief van 1 september 2025 zijn de aanvullend getroffen maatregelen beschreven. Het belangrijkste is dat er zo snel mogelijk duidelijkheid komt uit de verschillende onderzoeken naar hoe deze hack heeft kunnen plaatsvinden en op welke wijze verdere maatregelen ter bescherming van dataveiligheid nodig zijn. Zodra relevante uitkomsten van de onderzoeken bekend zijn, zal ik uw Kamer daarover informeren.

Vraag 2
Is het duidelijk welke gegevens er van de 485.000 gedupeerden precies buitgemaakt zijn? Gaat u hen direct informeren over welke gegevens per persoon zijn buitgemaakt of al zijn gelekt?

Antwoord 2
Welke gegevens van de getroffenen van de hack precies bemachtigd zijn, is op individueel niveau nu nog niet te zeggen. Indien hier meer duidelijkheid over komt, wordt bekeken hoe deelnemers hier zo goed mogelijk over geïnformeerd kunnen worden. BVO NL weet inmiddels wel op persoonsniveau welke gegevens er per deelnemer met het laboratorium zijn gedeeld en zal alle getroffenen daarover nader informeren, ook de getroffenen die in de week van 18 augustus al een brief
ontvangen hebben. Deze brieven worden naar verwachting halverwege september verstuurd. Ik heb uw Kamer in mijn brief van 1 september 2025 ook geïnformeerd over welke gegevens door BVO NL met het laboratorium zijn gedeeld.

Vraag 3
Hoe borgt u dat de communicatie richting burgers begrijpelijk, meertalig en toegankelijk is? Kunt u bovendien garanderen dat trans- en non-binaire personen die zijn gedupeerd met de juiste of een neutrale aanhef worden aangeschreven?

Antwoord 3
Er wordt door BVO NL extra aandacht besteed aan de begrijpelijkheid van de brieven die medio september worden verzonden. De signalen en feedback hierover op de brieven die in de week van 18 augustus zijn verzonden, worden meegenomen in deze nieuwe ronde brieven. BVO NL betrekt hierin ook het RIVM. Het RIVM werkt al langer aan het vergroten van de toegankelijkheid van de bevolkingsonderzoeken naar kanker en kan die expertise dus goed inbrengen. Ik heb ook een brief ontvangen van de Nationale ombudsman over informatievoorziening rond de hack. Ik heb deze brief gedeeld met BVO NL, zodat zij met de suggesties en opmerkingen van de ombudsman aan de slag kunnen voor deze nieuwe ronde brieven. Ook ga ik op basis van de brief van de ombudsman in gesprek met de betrokken partijen om samen te bepalen welke aanvullende acties mogelijk zijn.
De brieven van BVO NL worden alleen in het Nederlands opgesteld, omdat BVO NL niet weet wie welke taal spreekt. BVO NL zal de brieven wel in het Nederlands en Engels op hun website plaatsen. Wat betreft de aanhef in de reeds verzonden brieven, geldt dat BVO NL zich realiseert dat de woordkeuze («mevrouw») niet de ervaring en identiteit vertegenwoordigt van iedereen in de doelgroep van het bevolkingsonderzoek. Om die reden wordt voor de nieuwe ronde brieven verkend welke technische mogelijkheden er zijn om de aanhef meer op maat te kiezen. Mocht dit niet mogelijk zijn, zal BVO NL hier op een alternatieve manier aandacht aan besteden in de brief.

Vraag 4
Kunt u nader ingaan op de directe gevolgen van het lek voor de gedupeerden? Hoe wordt hun gestolen data vermoedelijk gebruikt?

Antwoord 4
De grootste risico's van de hack bij het laboratorium voor burgers zijn phishing en identiteitsfraude.
Door phishing in e-mails, per sms of telefoon kunnen criminelen proberen burgers te verleiden tot het delen van wachtwoorden of geven van informatie. Een andere mogelijkheid is dat door op een link te klikken malware wordt geïnstalleerd op de computer, telefoon of het netwerk. Dit kan leiden tot schade aan IT-systemen, tot spionage of tot nieuwe datadiefstal.

Wanneer criminelen beschikken over persoonsgegevens kunnen ze zich voordoen als iemand anders en identiteitsfraude plegen.

Vraag 5
Hoeveel burgers hebben contact opgenomen met het klantcontactcentrum van Bevolkingsonderzoek Nederland? Is er voldoende capaciteit om vragen en zorgen goed af te handelen? Zo niet, bent u bereid hier middelen voor vrij te maken?

Antwoord 5
Er komen begrijpelijkerwijs veel vragen binnen bij het klantcontactcentrum van BVO NL. Het betreft circa 80 tot 400 telefoontjes per dag, en circa 2.000 ontvangen e-mails in de periode tot en met 1 september 2025. De hoeveelheid vragen op een dag is afhankelijk van de actualiteiten, zoals berichtgeving in de media. De capaciteit bij het klantcontactcentrum is opgeschaald. Er is op dit moment voldoende capaciteit om de vragen aan te kunnen. Het klantcontactcentrum is uitgebreid met een speciale informatielijn (0800-1617) met specialisten op het gebied van crisistelefonie.
Mijn prioriteit is om BVO NL in staat te stellen om de gevolgen van de hack zo goed als mogelijk te beperken voor alle betrokkenen. Op dit moment is er geen zicht op of dit financiële gevolgen heeft voor VWS en/of de uitvoeringsorganisaties.

Vraag 6
Welke maatregelen kunnen gedupeerden treffen om zich te beschermen tegen misbruik van hun gegevens? Hoe gaat u direct met hen communiceren om daarin te helpen?

Antwoord 6
Het advies voor de mensen die een brief van BVO NL hebben gekregen dat hun gegevens onderdeel zijn geweest van de hack bij het laboratorium, is om extra alert te zijn op vreemd gebruik van persoonlijke gegevens. Het gaat dan met name om nepmail, neptelefoontjes, vreemde sms-berichten of misbruik van persoonsgegevens (identiteitsfraude). Op de website van de Rijksoverheid wordt meer informatie gegeven hoe deze situaties herkend kunnen worden en hoe hiervan melding gedaan kan worden. Bij vragen, ongerustheid en/of andere opmerkingen kunnen deelnemers terecht bij het klantcontactcentrum van BVO NL.

Vraag 7
Met hoeveel zekerheid kunt u zeggen dat de gestolen gegevens daadwerkelijk niet verder worden verspreid of verkocht? Hoe monitort u de verdere verspreiding van deze gegevens om in kaart te brengen wie de gelekte gegevens mogelijk in handen hebben?

Antwoord 7
Ik heb geen zekerheid over wat criminelen met de gegevens doen die zij hebben buitgemaakt. Zodra persoonsgegevens eenmaal op het dark web zijn beland, is het in de praktijk bijzonder lastig, zo niet onmogelijk, om deze volledig te laten verwijderen. Het dark web betreft een afgeschermd deel van het internet waar informatie vaak anoniem wordt gedeeld en waar activiteiten lastig tot niet te traceren zijn. Z-CERT heeft aangegeven dat er tijdelijk een deelverzameling is gepubliceerd op het dark web. Deze deelverzameling kan in de periode dat deze online stond, door anderen ingezien of gekopieerd zijn. De gehele dataset die in handen zou zijn gekomen van de hackergroep kan op een later moment ook alsnog door hen misbruikt worden.
Politie en OM doen onderzoek naar de hack bij het laboratorium. Ik hoop dat de daders gevonden worden en de gestolen dataset gewist wordt.
Z-CERT monitort of de data (opnieuw) op het darkweb verschijnt en onderneemt in dat geval actie.

Vraag 8
Kunt u aangeven of de verwerkersovereenkomsten[4] tussen Bevolkingsonderzoek Nederland en Clinical Diagnostics volledig op orde waren? Bent u bereid deze overeenkomsten (geanonimiseerd) met de Kamer te delen?

Antwoord 8
Op grond van de AVG is het sluiten van een verwerkersovereenkomst verplicht als een verwerking namens en in opdracht van een verwerkingsverantwoordelijke wordt verricht door een verwerker. Een verwerkersovereenkomst moet in ieder geval afspraken bevatten over de onderwerpen die de AVG voorschrijft. Die onderwerpen betreffen onder meer de aard, het doel en de duur van de verwerking. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van deze verplichtingen uit de AVG. Indien in dit concrete geval een verplichting bestond om een verwerkingsovereenkomst te sluiten, is het aan de AP om te beoordelen of de inhoud daarvan aan de eisen van de AVG voldoet. De AP is reeds een onderzoek gestart.

Vraag 9
Kunt u aangeven of er toezicht is geweest op het technisch voldoen aan minimale beveiligingseisen[5] om de basisbeveiliging te borgen? Zo ja, hoe is het bij de hack alsnog verkeerd gegaan? Zo niet, gaat u naleving alsnog verplichten en de organisaties hierbij helpen?

Antwoord 9
De diverse aspecten waarnaar gevraagd wordt, moeten blijken uit de verschillende lopende onderzoeken naar de hack en het datalek dat daarop volgde.
In het algemeen geldt dat op het gebied van de informatiebeveiliging in de zorg er sectorspecifieke wet- en regelgeving is (onder andere de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en de Wet kwaliteit, klachten en geschillen zorg (Wkkgz)). De IGJ is belast met het toezicht op de naleving van die wet- en regelgeving. Zorgorganisaties zijn verantwoordelijk voor de implementatie van technische maatregelen en de controle daarop.
De IGJ heeft mij laten weten dat dit laboratorium nog niet eerder bezocht is in het kader van informatieveiligheid. De IGJ heeft inmiddels aangekondigd onderzoek te doen bij het laboratorium en is voornemens om mede naar aanleiding van dit incident extra aandacht te besteden aan informatiebeveiliging bij medische laboratoria. Risico's zoals deze blijken uit dit incident, worden eveneens meegenomen in het toezicht bij andere zorgaanbieders en andere zorgsectoren.
Daarnaast geldt dat de Minister van Justitie en Veiligheid het wetsvoorstel Cyberbeveilingswet (Cbw) op 2 juni 2025 aanhangig heeft gemaakt in uw Kamer. Dit wetsvoorstel zal, indien beide Kamers der Staten-Generaal daarmee instemmen, ook gaan gelden voor zorgaanbieders in Nederland die voldoen aan de eisen voor wat betreft de omvang van de organisatie. Deze zorgaanbieders en zorgketenorganisaties krijgen met de Cbw een zorgplicht met betrekking tot informatieveiligheid. Deze zorgplicht geldt ook voor uitbestede diensten. Daarnaast komt er een incidentmeldplicht richting de toezichthouder IGJ en richting Z-CERT, die ondersteuning geeft aan en een actieve waarschuwingsdienst opzet voor deze zorg- en zorgketenorganisaties (met name op het gebied van scanning en dreigingsanalyse). Voornoemde meldplicht aan de IGJ en Z-CERT bestaat in de huidige situatie nog niet. Ook de handhavingsmogelijkheden onder de Cbw gaan verder dan onder de Wabvpz.

[4] Dit betreft ook bepalingen over NEN 7510/ USI 27001, auditrechten, boetebepalingen en incident-SLA's.
[5] Dit betreft o.a. het toezien dat er penetratietesten worden uitgevoerd en het verplichten van gestandaardiseerd onderzoek volgens de Methodiek voor Informatiebeveiligingsonderzoek met Auditwaard (MIAUW).

Vraag 10
Bent u bereid om de NEN 7510, ISAE 3000 en vergelijkbare standaarden standaard op te nemen in de inkoopeisen van het Ministerie van Volksgezondheid, Welzijn en Sport? Ziet u dit als een noodzakelijke stap om beter inzicht te krijgen in de cyberveiligheid van betrokken organisaties?

Antwoord 10
Ja. Het Ministerie van VWS hanteert bij de inkoop en uitbesteding van ICT-diensten het rijksbrede normenkader voor informatiebeveiliging, de Baseline Informatiebeveiliging Overheid (BIO). De BIO is gebaseerd op internationale standaarden, zoals ISO/IEC 27001 en ISO/IEC 27002 en bevat specifieke aanvullende overheidsmaatregelen.
Voor leveranciers die persoonsgegevens verwerken geldt aanvullend de norm NEN 7510. Deze norm is wettelijk verankerd in de zorgsector en kan door VWS contractueel worden verlangd van leveranciers die dergelijke gegevens verwerken.
Daarnaast wordt bij contracteren, waar passend, gevraagd om assurancerapportages, bijvoorbeeld de ISAE 3000 of SOC-rapporten, waarmee leveranciers aantoonbaar maken dat zij de gestelde beveiligingsmaatregelen in de praktijk hebben ingericht en effectief laten functioneren.
In lijn met de aankomende Cyberbeveiligingswet (implementatie van NIS2) en de BIO 2.0 wordt leveranciersmanagement verder versterkt, onder meer door het stellen van expliciete eisen aan ketenbeveiliging, incidentmeldingen en onafhankelijke toetsing. Hiermee wordt geborgd dat VWS zijn verantwoordelijkheid neemt voor de beveiliging van uitbestede processen en de bescherming van gegevens in de zorg- en Rijkscontext.

Vraag 11
Welke concrete eisen gaat u stellen aan dataminimalisatie en -retentie bij bevolkingsonderzoeken en laboratoria, zoals tokenisatie, pseudonomisering en kortere bewaartermijnen?

Antwoord 11
Het is van groot belang dat bij de verwerking van bijzondere persoonsgegevens zoals medische persoonsgegevens, aan de wettelijke vereisten wordt voldaan. Het gaat in ieder geval om de beginselen inzake de verwerking van persoonsgegevens die zijn neergelegd in artikel 5 AVG (o.a. rechtmatigheid, transparantie, doelbinding en het principe van dataminimalisatie). Aanvullende (informatiebeveiligings)normen gelden ingeval van verwerking van persoonsgegevens met een hoog risico voor rechten en vrijheden van burgers. Het is aan de organisatie die verantwoordelijk is voor verwerking van persoonsgegevens (de verwerkingsverantwoordelijke) om aan te tonen dat zij voldoet aan de toepasselijke normen en uiteindelijk aan de AP om te beoordelen of dat het geval is (geweest). Dat geldt dus ook voor bevolkingsonderzoeken en laboratoria.

Vraag 12
Wanneer verwacht u de uitkomsten van de aangekondigde onderzoeken door Bevolkingsonderzoek Nederland, de RIVM en de Autoriteit Persoonsgegevens? Welke duidelijkheid moeten deze onderzoeken verschaffen?

Antwoord 12
BVO NL laat verschillende onderzoeken uitvoeren met als doel om:
– de oorzaak en omvang van de hack vast te stellen;
– onafhankelijk vast te stellen welke gegevens van deelnemers aan het bevolkingsonderzoek precies buit zijn gemaakt;
– (acute) risico's bij de bevolkingsonderzoeken te inventariseren;
– een evaluatie uit te voeren naar de huidige beveiligingsmaatregelen;
– terug te blikken op gemaakte keuzes in datastromen, opslag en bewaartermijnen.

Zoals ook aangegeven in het antwoord op vraag 1 is het belangrijk dat er zo snel mogelijk duidelijkheid komt op basis van de verschillende onderzoeken. Op dit moment is er nog geen precieze planning te geven. Op het moment dat dat wel het geval is, zal uw Kamer daarover geïnformeerd worden. Ook de AP en de IGJ kunnen nog niet aangeven wanneer hun onderzoeken

gereed zijn, omdat niet te voorzien is wat ze tegenkomen en waar nader onderzoek naar nodig is.

Vraag 13
Hoe zorgt u ervoor dat organisaties leren van de hack en de uitkomsten van alle onderzoeken worden gebruikt om de bescherming van persoonsgegevens bij essentiële organisaties feitelijk te verbeteren? Via welke structuren gaat u deze kennisuitwisseling faciliteren?

Antwoord 13
Digitale veiligheid vormt een essentieel aandachtspunt vormt voor de gehele maatschappij. In (bestuurlijke) gesprekken met partners uit het veld wordt dataveiligheid door het Ministerie van VWS actief onder de aandacht gebracht. In het zorgveld zijn een aantal manieren om te leren van incidenten:
– In het Zorg Detectie Netwerk werkt Z-CERT nauw samen met diverse IT-security bedrijven. Deze bedrijven delen via het Zorg Detectie Netwerk zorgspecifieke dreigingsinformatie en informatie over kwetsbaarheden met hun klanten uit de zorgsector. Andere deelnemers leren zo van incidenten en worden gewaarschuwd. Ook deelt Z-CERT elk kwartaal een dreigingsanalyse met alle deelnemende zorgorganisaties.
– De lessen die volgen uit de onderzoeken die BVO NL heeft ingesteld, zal ik breder delen.
– Ik faciliteer het Platform voor informatiebeveiliging en privacy (IV&P). deze overlegstructuur, is bedoeld voor koepels en branches om ideeën en ervaringen op te halen en kennis uit te wisselen. Daarnaast worden actualiteiten geduid en risico's uit de praktijk gesignaleerd.
– Z-CERT produceert kennisproducten, adviezen en waarschuwingen en geeft webinars over geleerde lessen uit incidenten.

Vraag 14
Heeft u meer organisaties geïdentificeerd die op eenzelfde manier kwetsbaar zijn voor een hack van zo'n ordegrootte? Welke concrete maatregelen neemt u om hun cyberveiligheid in orde te brengen zodat een soortgelijk datalek niet meer kan gebeuren?

Antwoord 14
Ik heb op dit moment geen signalen dat andere organisaties ook kwetsbaar zijn voor een hack zoals bij dit laboratorium heeft plaatsgevonden. Zorgaanbieders zijn in de eerste plaats zelf wettelijk verantwoordelijk voor hun informatieveiligheid en het voorkomen van datalekken. Dat neemt niet weg dat ik me ook inzet voor het verkleinen van de risico's en de impact hiervan. Dit doe ik door te zorgen voor meer bewustwording met het programma informatieveilig gedrag in de zorg, duidelijke normen en kaders te stellen en door hulpmiddelen aan te bieden om deze te implementeren. Daarnaast biedt Z-CERT gespecialiseerde ondersteuning aan zorgaanbieders. Z-CERT monitort continu de systemen die benaderbaar zijn via het internet van de bij hen aangesloten zorgaanbieders en informeert deze zorgaanbieders over mogelijke risico's in hun cyberbeveiliging. Daarnaast adviseert Z-CERT zorg- en zorgketenorganisaties over maatregelen die de cyberweerbaarheid verhogen en stelt adviezen hiervoor op hun website beschikbaar. Zo zijn onder meer de tien belangrijkste maatregelen tegen ransomwaredreiging op hun website geplaatst.

Vraag 15
Kunt u deze vragen los van elkaar en zo snel mogelijk beantwoorden?

Antwoord 15
De vragen zijn zo snel als mogelijk beantwoord.