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

2963

Vragen van de leden **Hertzberger** en **Six-Dijkstra** (beiden Nieuw Sociaal Contract) aan de Minister en Staatssecretaris van Volksgezondheid, Welzijn en Sport, de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid over *het datalek van medische en persoonlijke gegevens bij het laboratorium van Clinical Diagnostics in Rijswijk* (ingezonden 13 augustus 2025).

Antwoord van Staatssecretaris **Tielen** (Volksgezondheid, Welzijn en Sport), mede namens de Minister van Volksgezondheid, Welzijn en Sport (ontvangen 1 september 2025).

Vraag 1
Hoe bestaat het dat het anno 2025, in tijden dat we maximaal weerbaar moeten zijn, mogelijk is om bij een zorgpartij van een half miljoen Nederlanders uiterst gevoelige medische gegevens en persoonsgegevens te stelen?

Antwoord 1
Bevolkingsonderzoek Nederland (BVO NL) heeft een onafhankelijk onderzoek ingesteld naar de exacte omvang en de oorzaak van deze hack. Ook de Autoriteit Persoonsgegevens (AP) en de Inspectie Gezondheidszorg en Jeugd (IGJ) zijn een onderzoek gestart. Los daarvan markeer ik hierbij het grote belang van adequate technische en organisatorische maatregelen ter beveiliging van persoonsgegevens, in het bijzonder als het gaat om gezondheidsgegevens. Zorgaanbieders zijn daartoe wettelijk verplicht, onder andere op grond van de Algemene verordening gegevensbescherming (AVG). Ik betreur het dan ook ten zeerste dat gezondheidsgegevens zijn bemachtigd bij een hack bij Clinical Diagnostics.

Vraag 2
Wanneer werd het datalek bekend bij de Stichting Bevolkingsonderzoek Nederland en bij het Ministerie van Volksgezondheid, Welzijn en Sport? Kunt u een tijdlijn maken met de belangrijkste gebeurtenissen en wanneer zij ontdekt zijn? Kunt u daarop zeggen wanneer de diefstal plaatsvond, wanneer mensen en de Autoriteit Persoonsgegevens geïnformeerd zijn, wanneer het ministerie/de bewindspersonen geïnformeerd zijn en alle andere relevante gebeurtenissen?

ah-tk-20242025-2963
ISSN 0921 - 7398
's-Gravenhage 2025

Antwoord 2
BVO NL is op woensdag 6 augustus door het laboratorium Clinical Diagnostics geïnformeerd over de hack, nadat het laboratorium de hack op 6 juli heeft ontdekt. BVO NL heeft op 6 augustus een melding gemaakt bij de AP en heeft op dezelfde dag het RIVM, de opdrachtgever van BVO NL, geïnformeerd. Het Ministerie van VWS is op donderdag 7 augustus geïnformeerd door het RIVM. BVO NL heeft op zaterdag 9 augustus een melding gedaan bij de IGJ. Op maandag 11 augustus heeft BVO NL een nieuwsbericht uitgebracht over de hack en is uw Kamer geïnformeerd. Op maandag 11 augustus heeft ook Z-Cert, het expertisecentrum voor cybersecurity in de zorg, bij het Ministerie van VWS melding gemaakt over de hack.
In de week van 18 augustus heeft BVO NL de eerste groep deelnemers waarvan vaststaat dat zij betrokken zijn bij de hack, per brief geïnformeerd. Nadien heeft het laboratorium desgevraagd aan mij aangegeven dat het onderzoek naar de aantallen bijna is voltooid en dat de betrokken zorgaanbieders nader zullen worden geïnformeerd.
Zoals ik vrijdag 29 augustus en vandaag in aparte brieven aan uw Kamer heb laten weten, blijkt uit dit onderzoek dat nog meer deelnemers aan het bevolkingsonderzoek zijn getroffen door de hack. BVO NL heeft hier op 29 augustus ook een nieuwsbericht over gepubliceerd. Deze deelnemers ontvangen van BVO NL een brief.

Vraag 3
Waarom wordt het lekken van persoonlijke en medische gegevens van een half miljoen Nederlanders pas meer dan vier weken later openbaar gemaakt? Klopt het dat er al eerder een lek bij dit laboratorium was gesignaleerd maar daar niet naar werd gehandeld, er geen consequenties waren?

Antwoord 3
In situaties als deze rust op verwerkingsverantwoordelijken de verplichting datalekken aan de AP en betrokkenen te melden binnen de termijnen die de Algemene Verordening Gegevensbescherming (AVG) noemt. Of en waarom dat hier niet gebeurd zou zijn, is ter beoordeling van de AP die inmiddels een onderzoek is gestart.

Vraag 4
Bent u het ermee eens dat dit het vertrouwen van Nederlanders in het bevolkingsonderzoek, waar al steeds minder in wordt deelgenomen, ernstig ondermijnt?

Antwoord 4
Ik begrijp heel goed dat (potentiële) deelnemers aan het bevolkingsonderzoek zich zorgen maken en vragen hebben na het bericht over de hack. Meedoen aan een bevolkingsonderzoek kan al spanning met zich meebrengen. Als je dan ook nog hoort dat je persoonsgegevens mogelijk zijn bemachtigd, is dat een ontzettende schok. Deelnemers aan bevolkingsonderzoeken moeten er immers op kunnen vertrouwen dat hun persoonlijke gegevens veilig zijn. Dat er nu persoonlijke gegevens zijn gestolen door hackers, vind ik ontzettend betreurenswaardig. Ik kan me voorstellen dat dit mensen aan het denken zet over deelname aan het bevolkingsonderzoek. Ikwil benadrukken dat het vroeg opsporen van kanker ervoor zorgt dat de behandeling minder belastend is en een betere uitkomst heeft, waardoor sterfgevallen door de betreffende vorm van kanker voorkomen worden. Deelname is dus in ieders belang.

Vraag 5
Hoe kan het dat er met één hack zoveel gegevens van zoveel mensen in één keer buit kunnen worden gemaakt? Waarom worden medische uitslagen in combinatie met burgerservicenummers en adresgegevens opgeslagen? Wordt er in deze laboratoria gewerkt met het gespreid en versleuteld opslaan van een minimaal benodigde hoeveelheid gegevens? Welke concrete inspanningen worden er geleverd om te voldoen aan het beginsel van dataminimalisatie conform artikel 5 AVG?

Antwoord 5
De diverse aspecten waarnaar gevraagd wordt, moeten blijken uit de verschillende lopende onderzoeken naar de hack en het datalek dat daarop volgde.
In algemene zin markeer ik het grote belang dat bij de verwerking van bijzondere persoonsgegevens zoals medische persoonsgegevens aan de wettelijke vereisten wordt voldaan, waaronder in ieder geval 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).

Vraag 6
Valt dit lab, één van de grootste van Nederland, onder toezicht van de Inspectie Gezondheidszorg en Jeugd (IGJ)? Zo ja, wanneer heeft de Inspectie voor het laatst dit laboratorium bezocht en wat waren toen de bevindingen?

Antwoord 6
Op het gebied van de informatiebeveiliging in de zorg is er sectorspecifieke wet- en regelgeving (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.
De IGJ heeft mij laten weten dat dit laboratorium nog niet eerder bezocht is in het kader van informatieveiligheid. De IGJ is inmiddels een onderzoek gestart bij het laboratorium en is voornemens om mede naar aanleiding van dit incident extra aandacht te besteden aan informatiebeveiliging bij medische laboratoria.

Vraag 7
Wat zijn de minimumvereisten voor dataveiligheid van Stichting bevolkingsonderzoek? Aan welke standaarden moeten laboratoria voldoen om grootschalig labonderzoek te mogen verrichten?

Antwoord 7
Wat betreft de eerste vraag geldt dat voor zover BVO NL persoonsgegevens verwerkt ten aanzien waarvan BVO NL geldt als verwerkingsverantwoordelijke, BVO NL zich in ieder geval moet houden aan de AVG. Op grond van de AVG dient BVO NL in dat geval organisatorische en technische maatregelen te treffen ter beveiliging van persoonsgegevens. De AP houdt hierop toezicht. Daarbij betrekt het informatiebeveiligingsnormen als de NEN7510. Die normen gelden als gezaghebbende uitwerking van de algemene beveiligingsnorm uit de AVG. Die sectorspecifieke informatiebeveiligingsnormen zijn voor zorgaanbieders overigens verplicht gesteld in het Besluit elektronische gegevensverwerking door zorgaanbieders.
Wat betreft de tweede vraag geldt dat voor laboratoria wet- en regelgeving op het gebied van kwaliteit van de zorg en dataveiligheid kan gelden. Welke wet- en regelgeving dat precies betreft, hangt af van de concrete omstandigheden (zoals de aard van de werkzaamheden). De schaalgrootte van de labonderzoeken speelt hierbij in principe geen rol.

Vraag 8
Hoe was het gesteld met de datahuishouding en -veiligheid bij dit lab? Beschikte het laboratorium over de NEN 7510 certificering voor databeveiliging? Klopt het dat alle zorgpartijen die met bijzondere persoonsgegevens werken verplicht zijn om aan de NEN7510 richtlijn te voldoen? Voldeed dit lab hieraan? Gaan medische laboratoria onder de NIS-2 wetgeving vallen?

Antwoord 8
Het antwoord op deze vragen zal voortvloeien uit de verschillenden lopende onderzoeken naar de hack en het datalek. Algemeen geldt, in het kader van goede en veilige zorg, dat zorgaanbieders die persoonsgegevens verwerken

in een zorginformatiesysteem, moeten kunnen laten zien dat ze werken volgens de daarvoor geldende informatiebeveiligingsnormen, waaronder de NEN 7510. De IGJ houdt hier toezicht op en de AP, voor zover het gaat om de bescherming van persoonsgegevens.
Er bestaat binnen de NIS2-richtlijn of het wetsvoorstel Cyberbeveilingswet (Cbw), dat de Minister van Justitie en Veiligheid op 2 juni 2025 aanhangig heeft gemaakt in uw Kamer, geen categorie die zich specifiek richt op medische laboratoria. Een medisch laboratorium zou onder de NIS2-richtlijn kunnen vallen indien het bijvoorbeeld handelingen uitvoert die vallen onder de Wkkgz of wanneer het (deels) onderzoek doet naar geneesmiddelen en voor zover zij voldoen aan de eisen in de NIS-2-wetgeving op het gebied van omvang personeelsbestand en omzet. Het hangt dus af van de dienstverlening of een medisch laboratorium onder een van de categorieën van de NIS2-richtlijn of Cbw valt.

Vraag 9
Worden er vandaag nog steeds samples gestuurd vanuit het bevolkingsonderzoek of andere medische diagnostiek naar laboratoria waar deze data niet veilig zijn en worden verwerkt door systemen die niet aan de richtlijnen voldoen?

Antwoord 9
BVO NL heeft de samenwerking met het laboratorium tot nader order opgeschort. Bij de andere laboratoria betrokken bij de bevolkingsonderzoeken worden door Z-Cert extra checks gedaan op informatieveiligheid.

Vraag 10
Bij hoeveel Eurofins laboratoria speelt dit? Bij hoeveel andere medische laboratoria?

Antwoord 10
Er zijn bij mij geen signalen bekend dat de informatiebeveiliging bij andere laboratoria niet op orde zou zijn.

Vraag 11, 12 en 13
Welke andere zorgpartijen beschikken over de medische en persoonsgegevens van honderdduizenden Nederlanders zonder dat de dataveiligheid op orde is?
Op welke termijn kunt u dit in kaart brengen?
Wat bent u van plan om te doen als blijkt dat deze onveilige situatie bij andere zorgpartijen speelt?

Antwoord 11, 12 en 13
Ik heb geen inzicht in de hoeveelheid gezondheidsdata waar de verschillende zorgpartijen over beschikken. De zorg digitaliseert in toenemende mate en dit brengt grote voordelen met zich mee, maar ook risico's. Zorgpartijen zijn verantwoordelijk voor informatieveiligheid. Zij zijn verplicht te voldoen aan de wettelijke normen voor informatiebeveiliging in de zorg.
Zorginstellingen zijn in de eerste plaats zelf verantwoordelijk om de risico's te beperken en de impact van incidenten zo klein mogelijk te maken wanneer deze toch plaatsvinden. Dit neemt echter niet weg dat ik me ook inzet op 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, door duidelijke normen en kaders te stellen en door hulpmiddelen aan te bieden om deze te implementeren. Daarnaast biedt Z-Cert gespecialiseerde ondersteuning aan zorgaanbieders.

Vraag 14
Wat verwacht u van de effecten van dit massale datalek voor de veiligheid van Nederlanders en hoe beoordeelt u de risico's op onder andere identiteitsfraude, chantage of zorgmijden als gevolg hiervan? Hoe worden mensen met gevoelige adresgegevens, zoals penitentiaire inrichtingen, blijf-van-mijn-lijf-huizen en psychiatrische klinieken geholpen?

Antwoord 14
Hacks waarbij zoveel data worden bemachtigd vergroten het risico op gerichte en overtuigende phishingaanvallen, juist omdat kwaadwillende beschikken over persoonlijke informatie waarvan het slachtoffer zich mogelijk niet bewust is dat deze is buitgemaakt.
BVO NL informeert de getroffen deelnemers van het bevolkingsonderzoek baarmoederhalskanker. In de brief van BVO NL wordt ook gewezen op het risico op fraude. De betrokken (ex-)gedetineerden worden via een informatiebrief van Clinical Diagnostics over de hack geïnformeerd, met daarbij een begeleidende brief van de Dienst Justitiële Inrichtingen (DJI). In deze brieven is onder meer opgenomen wat betrokkenen kunnen doen.

Vraag 15
Kunt u deze vragen los van elkaar, zo snel mogelijk en zeker binnen drie weken beantwoorden?

Antwoord 15
Daar zet ik mij voor in.