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

2964

Vragen van het lid **Joseph** (BBB) aan de Minister en Staatssecretaris van Volksgezondheid, Welzijn en Sport over *het artikel «Datahack bij laboratorium veel groter, deel gegevens op dark web»* (ingezonden 12 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
Kunt u bevestigen dat het datalek bij laboratorium Clinical Diagnostics veel groter blijkt dan eerder gemeld, en dat naast gegevens van 485 duizend vrouwen ook data van onderzoeken naar huid, urine, penis, anus en wondvocht zijn buitgemaakt?[1]

Antwoord 1
Het laboratorium Clinical Diagnostics heeft in zijn eerste berichtgeving over de hack aan Bevolkingsonderzoek Nederland (BVO NL) gemeld dat daarbij de gegevens van ruim 485.000 deelnemers van het bevolkingsonderzoek baarmoederhalskanker zijn bemachtigd. Zoals ik uw Kamer op vrijdag 29 augustus heb geïnformeerd, is duidelijk geworden dat er nog aanzienlijk meer deelnemers zijn getroffen door de hack. Namelijk ca. 230.000 mensen extra. Het is helaas niet uit te sluiten dat het hierbij blijft.
Uit contact met het laboratorium en Stichting Z-Cert (het expertisecentrum voor cybersecurity in de zorg) is naar voren gekomen dat de omvang van het datalek, naast de deelnemers van het bevolkingsonderzoek baarmoederhalskanker, inderdaad groter blijkt te zijn. Zo heeft de Staatssecretaris Rechtsbescherming uw Kamer geïnformeerd dat ook gegevens van 266 (ex-) gedetineerden betrokken zijn bij de hack.[2] Desgevraagd heeft het laboratorium aan mij aangegeven dat het onderzoek naar de aantallen bijna is voltooid en dat de betrokken zorgaanbieders nader zullen worden geïnformeerd.

[1] Nos.nl, 11 augustus 2025, «Datahack bij laboratorium veel groter, deel gegevens op dark web», (nos.nl/artikel/2578338-datahack-bij-laboratorium-veel-groter-deel-gegevens-op-dark-web).
[2] Brief van 21 augustus 2025, Kamerstuk II, 2024/25, 32 761, nr. 328.

ah-tk-20242025-2964
ISSN 0921 - 7398
's-Gravenhage 2025

Vraag 2
Hoe beoordeelt u het feit dat gegevens, inclusief burgerservicenummer, medische uitslagen en adviezen, deels op het dark web zijn verschenen en dat criminelen claimen 300 gigabyte aan data te hebben gestolen?

Antwoord 2
Ik betreur het ten zeerste dat persoonsgegevens van deelnemers aan het bevolkingsonderzoek baarmoederhalskanker zijn bemachtigd als gevolg van een hack bij het laboratorium Clinical Diagnostics. Bovenal voor de deelnemers die direct geraakt zijn door de hack, aangezien het grote impact kan hebben als je gegevens in verkeerde handen komen. Meedoen aan een bevolkingsonderzoek kan al spanning met zich meebrengen. Als je dan ook nog hoort dat je persoonsgegevens zijn bemachtigd bij een hack en mogelijk op het dark web zijn verschenen, is dat een ontzettende schok. Ook voor alle andere (potentiële) deelnemers aan de bevolkingsonderzoeken vind ik de situatie betreurenswaardig. Deelnemers aan de bevolkingsonderzoeken moeten er immers op kunnen vertrouwen dat hun persoonlijke gegevens veilig zijn. Ik begrijp heel goed dat zij zich zorgen kunnen maken en vragen hebben.
Ik vind het belangrijk dat deelnemers zo goed mogelijk worden geïnformeerd over de hack. Betrokken zijn of worden door BVO per brief geïnformeerd. Bij vragen, ongerustheid en/of andere opmerkingen kunnen deelnemers terecht bij het klantcontactcentrum[3] van BVO NL.

Vraag 3
Wat vindt u van het feit dat het datalek al op 6 juli 2025 bekend was bij het laboratorium, maar pas op 6 augustus 2025 is gemeld aan Bevolkingsonderzoek Nederland?

Antwoord 3
In situaties als deze rust op verwerkingsverantwoordelijken de verplichting datalekken aan de Autoriteit Persoonsgegevens (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
Kunt u bevestigen dat ook gegevens van patiënten van huisartsen en ziekenhuizen zoals het Leids Universitair Medisch Centrum, Amphia ziekenhuis en Alrijne ziekenhuis zijn gelekt? Wat betekent dit voor de verantwoordelijkheid van deze instellingen?

Antwoord 4
Uit contact met het laboratorium en Stichting Z-Cert is naar voren gekomen dat de omvang van het datalek inderdaad groter blijkt te zijn dan het bevolkingsonderzoek baarmoederhalskanker. Zoals ik afgelopen vrijdag en vandaag in aparte brieven uw Kamer heb laten weten, blijkt dat nog meer deelnemers aan het bevolkingsonderzoek zijn getroffen door de hack, ook deze deelnemers worden hierover door BVO NL geïnformeerd.
Desgevraagd heeft het laboratorium aan mij aangegeven dat het onderzoek naar de aantallen bijna is voltooid en dat de betrokken zorgaanbieders nader zullen worden geïnformeerd.

Vraag 5
Welke concrete maatregelen zijn inmiddels genomen om de schade voor betrokken burgers te beperken en herhaling te voorkomen?

Antwoord 5
Om meer inzicht te krijgen in de omvang van het probleem en om de gevolgen van de hack zoveel mogelijk te beperken, zijn de volgende maatregelen genomen:
– De samenwerking met het betreffende laboratorium is door BVO NL tot nader order opgeschort. Twee laboratoria die betrokken zijn bij het

[3] https://www.bevolkingsonderzoeknederland.nl/contact/

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.
– BVO NL heeft in afstemming met het RIVM een onderzoek ingesteld naar de exacte omvang en de oorzaak van deze hack.
– Er is onderzoek gestart naar wat BVO NL kan verbeteren aan onder meer dataminimalisatie, aanbestedingseisen en bewaartermijnen.
– 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.
– Het Openbaar Ministerie en de politie hebben bekend gemaakt strafrechtelijk onderzoek te doen naar het datalek.
– 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.
– Tot slot brengt het Ministerie van VWS databeveiliging permanent onder de aandacht in (bestuurlijke) gesprekken met partners uit het veld. Dataveiligheid is van ons allemaal en voor ons allemaal van groot belang. Het zou zo vanzelfsprekend moeten zijn als een brandverzekering. Dat vraagt op alle niveaus om alertheid, urgentie en inspanning: van de bestuurskamer tot de werkvloer. In technieken in gedrag. Ik zet mij in dat bewustzijn te vergroten, zeker in deze tijd van oplopende en voortdurende cyberdreigingen. Samen bouwen we daarmee aan het vertrouwen in databeschikbaarheid.

De komende periode beziet BVO NL op welke wijze de consequenties van de hack zoveel mogelijk kunnen worden beperkt. Ik sta hierover in nauw contact met het RIVM en BVO NL.
Van het laboratorium heb ik vernomen dat de betrokken zorgverleners en patiënten worden geïnformeerd en gewezen op de mogelijke risico's. Om herhaling te voorkomen heeft het laboratorium aanvullende maatregelen getroffen, waaronder het verder beperken van de toegang tot de getroffen IT-omgeving en verscherpte monitoring door het Security Operations Center (SOC)-team op de IT-omgeving.

Vraag 6
Hoe kan het dat Bevolkingsonderzoek Nederland en andere zorginstellingen geen gebruik maken van bijvoorbeeld Privacy by Design technieken, waardoor herleidbare persoonsgegevens niet uitgewisseld hoeven te worden tussen een extern laboratorium en de zorginstelling?

Antwoord 6
De diverse aspecten waarnaar gevraagd wordt, moeten blijken uit de verschillende lopende onderzoeken naar de hack en het datalek dat daarop volgde.

Vraag 7
Welke verbeteringen gaat u doorvoeren in het toezicht op digitale veiligheid bij laboratoria en andere zorginstellingen? Welke verbeteringen ziet u voor de lange termijn?

Antwoord 7
Digitale veiligheid vormt een essentieel aandachtspunt voor de gehele maatschappij. Op het gebied van de informatiebeveiliging in de zorg is er al 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 doet onderzoek 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). Deze meldplicht aan de IGJ bestaat in de huidige situatie nog niet. Ook de handhavingsmogelijkheden onder de Cbw gaan verder dan onder de Wabvpz.

Vraag 8
Hoe beoordeelt u de keuze om gezondheidsdata te laten beheren door private laboratoria? Kunt u toezeggen om te onderzoeken of centrale overheidsregie op digitale gezondheidsdata uitvoerbaar en wenselijk is?

Antwoord 8
Privacyregelgeving geldt voor iedereen, dus zowel voor publieke als private partijen. Vanuit dat oogpunt is er geen bezwaar om gezondheidsdata te laten beheren door private laboratoria.
Met betrekking tot het tweede aspect van uw vraag, het regievoeren op het organiseren van het gezondheidsinformatiestelsel, waar de organisatie van digitale gezondheidsdata een belangrijk onderdeel van is, gebeurt door het uitvoeren van de in april door de Tweede Kamer goedgekeurde Nationale Visie en Strategie (NVS) op het Gezondheidsinformatiestelsel[4]. In deze visie staat hoe de opslag en het beheer van digitale gezondheidsdata worden vormgegeven. Privacy en informatiebeveiligingseisen zijn een integraal onderdeel van de NVS, voor primaire zorginformatie en voor informatie zoals die gebruikt wordt voor het bevolkingsonderzoek.

Vraag 9
Bent u bekend met systemen waarbij data bij de bron wordt onthouden en pas bij verwijzing kunnen worden ingezien, met volledige logging van inzage? Hoe beoordeelt u de veiligheid van dit decentrale model ten opzichte van een centraal systeem zoals in Estland?

Antwoord 9
Ik ben bekend met de systemen waar u op doelt, het zogenoemde communicatiepatroon «gericht beschikbaar stellen», waarbij volledige logging van inzage plaats moet vinden. Ook in de situatie van laboratoriumonderzoek zou gebruik gemaakt kunnen worden van dit communicatiepatroon. Dit communicatiepatroon kan echter niet het hacken van data uit het laboratorium zelf voorkomen.
Met betrekking tot het tweede aspect van uw vraag, de inrichting van zorgstelsels in verschillende landen is niet altijd goed met elkaar te vergelijken. Veiligheidsvraagstukken en de afweging tussen centraal en decentraal worden meegenomen bij de inrichting van het gezondheidsinformatiestelsel op basis van de NVS.

Vraag 10
Is er inmiddels aangifte gedaan van deze hack? Zo ja, door wie en op welk moment? Is dit voor of na de melding op 6 augustus jl. aan Bevolkingsonderzoek Nederland? En mocht dit voor de melding op 6 augustus zijn geweest, hoe beoordeelt u de communicatie van organisaties bij datalekken, welke verbeteringen ziet u?

Antwoord 10
Over de vraag of er door direct betrokkenen aangifte is gedaan, kan ik mij niet uitlaten.

---

[4] Kamerstuk II, 2024/25, 27 529, nr. 326. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024Z21572&did=2024D50947

Vraag 11
Welke rol speelt de Inspectie Gezondheidszorg en Jeugd in het toezicht op digitale veiligheid bij laboratoria? Wordt deze rol versterkt?

Antwoord 11
Op het gebied van de informatiebeveiliging in de zorg is er sectorspecifieke wet- en regelgeving (onder andere de Wabvpz en Wkkgz). De IGJ is belast met het toezicht op de naleving van die wet- en regelgeving. De IGJ doet onderzoek 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.

Vraag 12
Wat kan de overheid nog doen als gegevens eenmaal op het dark web zijn verschenen, en hoe wordt de schade voor de betrokken burgers beperkt?

Antwoord 12
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.
Hoewel de mogelijkheden om schade volledig te voorkomen beperkt zijn, kunnen er door zorginstellingen wel maatregelen worden genomen om de (toekomstige) impact voor betrokkenen zoveel mogelijk te beperken. Een belangrijke stap is het tijdig informeren van betrokkenen zodra wordt vastgesteld dat hun gegevens op het dark web zijn aangetroffen. Hacks waarbij zoveel data worden bemachtigd, vergroten namelijk 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.
Door snel te informeren, kunnen betrokkenen proactief maatregelen nemen, zoals het wijzigen van wachtwoorden of het melden van mogelijke identiteitsfraude bij de daarvoor bestemde instanties (bijvoorbeeld bij de Rijksdienst voor Identiteitsgegevens[5]).

Vraag 13
Kunt u uitsluiten dat andere laboratoria of zorginstellingen eveneens slachtoffer zijn van deze of vergelijkbare hacks?

Antwoord 13
Zoals ik uw Kamer op vrijdag 29 augustus heb geïnformeerd, is duidelijk geworden dat er nog aanzienlijk meer deelnemers zijn getroffen door de hack. Namelijk ca. 230.000 mensen extra. Het is helaas niet uit te sluiten dat het hierbij blijft.
Desgevraagd heeft het laboratorium aan mij aangegeven dat het onderzoek naar de aantallen bijna is voltooid en dat de betrokken zorgaanbieders nader zullen worden geïnformeerd.
Z-Cert monitort continu de informatiebeveiliging van de bij hen aangesloten zorgaanbieders en informeert deze aanbieders over mogelijke risico's in hun informatiebeveiliging.

Vraag 14
Bent u bereid om een landelijke audit op databeveiliging bij zorginstellingen te laten uitvoeren, en daarbij ook de rol van de Autoriteit Persoonsgegevens, de Inspectie Gezondheidszorg en Jeugd en het Nationaal Cyber Security Centrum te betrekken?

[5] Centraal Meldpunt Identiteitsfraude (CMI) | RvIG

Antwoord 14
Nee, het is niet aan mij om landelijke audits uit te voeren. Zorginstellingen in Nederland zijn zelf verantwoordelijk en wettelijk verplicht voor het nemen van technische en organisatorische maatregelen ter bescherming van persoonsgegevens en medische informatie binnen hun organisatie. Zij dienen die maatregelen periodiek te evalueren en zo nodig aan te passen. De AP en de IGJ houden toezicht op de naleving van de betreffende regelgeving.
Bij de andere laboratoria betrokken bij de bevolkingsonderzoeken worden door Z-Cert extra checks gedaan op informatieveiligheid.

Vraag 15
Deelt u de mening dat het vertrouwen in bevolkingsonderzoeken ernstig wordt geschaad door dit datalek?

Antwoord 15
Ik begrijp heel goed dat (potentiële) deelnemers aan het bevolkingsonderzoek zich zorgen maken en vragen hebben na het bericht over deze 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. Ik wil 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 16
Welke maatregelen neemt u om het vertrouwen in bevolkingsonderzoeken te herstellen en deelname te stimuleren?

Antwoord 16
BVO NL onderneemt verschillende acties om de gevolgen van de hack zoveel mogelijk te beperken:
- 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.
- BVO NL heeft in afstemming met het RIVM een onderzoek ingesteld naar de exacte omvang en de oorzaak van deze hack.
- Er is onderzoek gestart naar wat BVO NL kan verbeteren aan onder meer dataminimalisatie, aanbestedingseisen en bewaartermijnen.
- 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.
- Het Openbaar Ministerie en de politie hebben bekend gemaakt strafrechtelijk onderzoek te doen naar het datalek.
- 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.
- Tot slot brengt het Ministerie van VWS databeveiliging permanent onder de aandacht in (bestuurlijke) gesprekken met partners uit het veld. Dataveiligheid is van ons allemaal en voor ons allemaal van groot belang. Het zou zo vanzelfsprekend moeten zijn als een brandverzekering. Dat vraagt op alle niveaus om alertheid, urgentie en inspanning: van de bestuurskamer tot de werkvloer. In technieken in gedrag. Ik zet mij in dat bewustzijn te vergroten, zeker in deze tijd van oplopende en voortdurende cyberdreigingen. Samen bouwen we daarmee aan het vertrouwen in databeschikbaarheid.

Ik verwacht dat deze acties bijdragen aan het behouden van vertrouwen in de bevolkingsonderzoeken.

Daarnaast lopen er momenteel verschillende pilots van het RIVM samen met BVO NL om de deelname aan de bevolkingsonderzoeken te stimuleren, waaronder een wijkgerichte aanpak, waarbij door een gezondheidsvoorlichter van het RIVM voorlichting wordt gegeven in wijkcentra in wijken waar de opkomst bij de bevolkingsonderzoeken laag is. Daarnaast wordt voorlichting gegeven op lokale evenementen en festivals en bij voedselbanken. Hierin wordt onder meer samengewerkt met gemeenten en GGD'en. Eventuele signalen die bij deze voorlichting naar voren komen wat betreft de informatievoorziening rond de hack, worden in overleg met BVO NL benut om de informatievoorziening vanuit BVO NL toegankelijker en begrijpelijker te maken.

Vraag 17
Hoe wordt de communicatie richting burgers afgestemd op de ernst van het datalek, en hoe worden deelnemers aan het bevolkingsonderzoek proactief geïnformeerd?

Antwoord 17
Op 11 augustus heeft BVO NL een nieuwsbericht naar buiten gebracht over de hack bij het laboratorium, om mensen te informeren en te waarschuwen. 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. In deze brief worden deelnemers onder andere geïnformeerd over het belang van alert zijn op fraude. Nu duidelijk is geworden dat meer deelnemers aan het bevolkingsonderzoek zijn getroffen, zullen ook deze deelnemers hierover door BVO NL worden geïnformeerd. Hierover heeft BVO NL op 29 augustus een nieuwsbericht gepubliceerd.
Op de website van BVO NL wordt de informatie voortdurend geüpdatet en worden veelgestelde vragen en antwoorden aangevuld. Bij vragen, ongerustheid en/of andere opmerkingen kunnen deelnemers terecht bij het klantcontactcentrum van Bevolkingsonderzoek Nederland. [6]

Vraag 18
Bent u bereid om met Gemeentelijke Gezondheidsdiensten, huisartsen en Bevolkingsonderzoek Nederland een herstelplan op te stellen voor het vertrouwen in preventieve zorg na dit incident?

Antwoord 18
Ik wacht op de uitkomsten van de lopende onderzoeken. Hieruit zullen lessen worden getrokken voor verbeteringen in de toekomst. Hierbij kijk ik ook zeker naar het vertrouwen in de preventieve zorg.

Vraag 19
Kunt u als Minister en Staatssecretaris, gezien de ernst van de situatie, toezeggen om voor 1 september 2025 uitgebreid antwoord te geven op bovenstaande vragen, inclusief een visie op de toekomst van digitale gezondheidsdata en cyberveiligheid in de preventieve zorg?

Antwoord 19
Met de Nationale Visie en Strategie voor het gezondheidsinformatiestelsel, zoals 14 april 2025 door Tweede Kamer akkoord bevonden, is een totaalvisie op het gezondheidsinformatiestelsel voor zorg, preventie en gezondheid gegeven. Mijn ministerie is nu druk bezig om deze visie te realiseren. Om die met vertrouwen van burger en zorgverlener te kunnen realiseren, zijn cyberveiligheid, privacy en informatiebeveiliging van wezenlijk belang en dus ook een integraal onderdeel van de strategie. Dit geldt voor zowel de primaire zorg en preventiezorg als voor gezondheidsdoeleinden.
De vragen zijn per 1 september beantwoord. Ik blijf uw Kamer op de hoogte stellen.

[6] https://www.bevolkingsonderzoeknederland.nl/contact/