Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

36 702 Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg

Nr. 9

NADER VERSLAG

Vastgesteld 22 januari 2026

De vaste commissie voor Volksgezondheid, Welzijn en Sport, belast met het voorbereidend onderzoek van voorliggend wetsvoorstel, heeft na kennisneming van de nota naar aanleiding van het verslag en de nota's van wijzigingen nog behoefte nadere vragen en opmerkingen aan de regering voor te leggen.

Onder het voorbehoud dat de in het nader verslag opgenomen vragen en opmerkingen afdoende door de regering worden beantwoord, acht de commissie de openbare behandeling van het wetsvoorstel voldoende voorbereid.

Inhoudsopgave **blz.**

I. Vragen en opmerkingen vanuit de fracties **1**
- Vragen en opmerkingen van de leden van de D66-fractie 1
- Vragen en opmerkingen van de leden van de VVD-fractie 3
- Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie 3
- Vragen en opmerkingen van de leden van de CDA-fractie 6
- Vragen en opmerkingen van de leden van de BBB-fractie 7
- Vragen en opmerkingen van de leden van de SGP-fractie 8

I. Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met belangstelling kennisgenomen van de wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg.

kst-36702-9
ISSN 0921 - 7371
's-Gravenhage 2026

De leden van de D66-fractie lezen in de memorie van toelichting vooral de positieve gevolgen van de invoering van de generieke functies voor identificatie en authenticatie, zoals uniformiteit, gebruiksgemak en een snellere registratie in het Dezi-register. Dezi staat voor «De Zorgidentiteit». Deze leden onderschrijven het belang daarvan, maar vragen of ook een expliciete inschatting is gemaakt van mogelijke obstakels voor patiënten en professionals in het zorg- en jeugdveld. Hoe worden zorg- en jeugdhulpaanbieders en hun medewerkers hierin praktisch ondersteund, en welke waarborgen zijn er om eventuele opstartproblemen tijdig te signaleren en te verhelpen zodat patiënten en professionals hier geen nadelige gevolgen van ondervinden?

De leden van de D66-fractie constateren dat het vereiste betrouwbaarheidsniveau «hoog» veel veiligheidsrisico's afdekt. Kan de regering echter specifiek aangeven welke risico's resteren na implementatie van dit niveau? Wie draagt de verantwoordelijkheid wanneer deze risico's zich materialiseren: de overheid (als stelselverantwoordelijke), de leverancier van het inlogmiddel, of de individuele zorgaanbieder?

De leden van de D66-fractie lezen dat het gebruik van persoonlijke apparaten voor digitale identificatie risico's met zich meebrengt, omdat het beheer (zoals beveiligingsupdates) niet bij de werkgever ligt. Hoe wordt voorkomen dat een inlogmiddel op niveau hoog toch onveilig wordt door malware op een slecht onderhouden privételefoon? Is het inlogmiddel in staat om te detecteren of een apparaat gehackt is (bijvoorbeeld door spionagesoftware) alvorens toegang te verlenen?

De leden van de D66-fractie lezen dat het risico op oneigenlijk gebruik van het burgerservicenummer (BSN) door zorgaanbieders bij de uitgifte van zorgspecifieke middelen wordt gecontroleerd door audits. Kan de regering concretiseren hoe vaak deze audits zullen plaatsvinden? Acht de regering een periodieke audit voldoende, of is er ook sprake van continu toezicht of steekproeven? Hoe wordt technisch en procedureel gegarandeerd dat het BSN daadwerkelijk direct en onherstelbaar uit de administratie van de middelenuitgever wordt verwijderd na de koppeling met het Dezi-nummer, en welke gevolgen treden er in werking bij het niet naleven van deze verwijderplicht?

De leden van de D66-fractie hebben vernomen dat er in contracten voor de hosting van het Dezi-register afspraken zijn gemaakt over de eventuele beëindiging van de dienstverlening van de hostingpartij. Wat staat er concreet in deze afspraken? Hoe wordt gegarandeerd dat bij een faillissement of contractbreuk van de commerciële hostingpartij de data van alle zorgverleners direct en veilig toegankelijk blijft zonder onderbreking van de zorg? Ook wordt er in het antwoord op de vraag van de collega's van de leden van de GroenLinks-PvdA-fractie geantwoord dat het Nederlands recht van toepassing is. Is er voldoende gewaarborgd dat deze data bij eventuele overnames door buitenlandse bedrijven nooit buiten de EU bewaard, ingezien of gebruikt kan worden?

De leden van de D66-fractie zijn op de hoogte van de komst van de EU Digital Identity Wallet (EUDI-wallet), naar verwachting in november 2026. Hoe wordt de technische en juridische aansluiting van het Dezi-stelsel op de EUDI-wallet exact vormgegeven? Betekent de Europese acceptatieplicht dat Nederlandse zorgaanbieders vanaf eind 2026 direct verplicht zijn om ook buitenlandse «wallets» van tijdelijke arbeidskrachten te accepteren, en zijn hun systemen daarop voorbereid?

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de eerste en tweede nota van wijziging. Zij hebben geen verdere vragen of opmerkingen aan de regering.

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de beantwoording op de vele vragen van de Kamerfracties. Echter hebben deze leden nog vragen en opmerkingen over de nota naar aanleiding van het verslag. Zij zetten deze per onderdeel uiteen.

Inleiding

De leden van de GroenLinks-PvdA-fractie vragen de regering om nader in te gaan op de pilot die de Ministeries van VWS en BZK met elkaar aan het voorbereiden zijn met betrekking tot de EU Digital Identity Wallet. Zij vragen de regering om te beschrijven wat het doel van deze pilot is en welke acties er ondernomen zullen worden om dit doel te bereiken.

Het huidige UZI-register en de inlogmiddelen

De leden van de GroenLinks-PvdA-fractie benadrukken nogmaals het belang van een cyberveilige zorgsector. De ketenrisico's binnen de zorg verdienen maximale aandacht. Met het op gang komen van nieuwe gegevensuitwisselingen als gevolg van dit wetsvoorstel, roept dit nog enkele vragen op. Zo zijn deze leden benieuwd hoe risico's worden voorkomen zoals het gebruiken van de nieuwe inlogmethoden op telefoons die geïnfecteerd zijn met ransomware, spyware of een dergelijk virus. Wordt naar aanleiding van dit wetsvoorstel ook meer aandacht gegeven aan het voorkomen van cyberveiligheidsrisico's onder zorgmedewerker? Deelt de regering de mening dat een toename in het gebruik van digitale inlogmiddelen gepaard moet gaan met een brede inzet op de digitale weerbaarheid van zorgmedewerkers? Zij vragen daarbij ook of de regering kan reflecteren op de rol van dit wetsvoorstel om datalekken te voorkomen. Er wordt gevraagd om in te schatten of, en zo ja hoeveel, cyberincidenten in 2025 voorkomen hadden kunnen worden als dit wetsvoorstel van kracht was geweest. Acht de regering de toename van kosten en administratieve lasten proportioneel aan de afname aan cyberveiligheidsrisico's in de zorg, als hier inderdaad sprake van is?

Medewerkers registreren in het Dezi-register

De leden van de GroenLinks-PvdA-fractie hebben vragen over de formulering van dit onderdeel van de wet. Gesproken wordt van zorgaanbieders die moeten verifiëren of een medewerker, die toegang vraagt tot een elektronische uitwisselingssysteem, «bij hem werkzaam is.» Echter lijkt dit niet van toepassing op zzp'ers of medewerkers die in een ander dienstverband voor een zorgaanbieder werkzaam zijn. Deze leden vragen de regering om te bevestigen of de toegang tot elektronische uitwisselingssystemen echt alleen maar van toepassing is op medewerkers die bij een zorgaanbieder werken, of ook voor mensen die voor een zorgaanbieder werken. Daarbij vragen ze ook om een nadere beschouwing van de gevolgen van dit wetsvoorstel op zzp'ers in de zorg.

De leden van de GroenLinks-PvdA-fractie hebben aanvullende vragen over de uitgifte van de nieuwe inlogmiddelen. In de beantwoording laat de regering weten dat het voor zorgaanbieders één tot twee dagen kan

duren om een certificaat van conformiteit met de NEN 7518 te verkrijgen. Er zijn echter gevallen waarin noodgedwongen externe inhuur wordt ingezet om uitgevallen medewerkers te vervangen. In het geval van acute inhuur zou met spoed een certificering aangevraagd moeten worden, wat ook werkdruk met zich meebrengt. Deze leden betwijfelen of dit realistisch gezien, kan worden verwacht van zorgaanbieders en hun personeel. Ook brengt het een risico mee dat er noodgedwongen gebruik wordt gemaakt van het inlogmiddel van de uitgevallen medewerker(s) die wordt/worden vervangen. Zij vragen daarom welke terugvalopties of tijdelijke middelen zorgaanbieders kunnen verwachten in het geval van acute inhuur, waarvoor één tot twee dagen aanvraagtijd te lang duurt. Ook vragen zij welke risico's de regering ziet, dat zulke casussen voorkomen. Is dit in de risico-inventarisatie meegenomen?

Geïnventariseerde risico's: het uitlenen van inlogmiddelen en gebruik privételefoon

De leden van de GroenLinks-PvdA-fractie hebben aanvullende vragen over het gebruik van privételefoons als inlogmiddel door zorgmedewerkers. Zij zien een cyberveiligheidsrisico door zorgdomeinen waarin (nog) geen of weinig gebruik wordt gemaakt van zakelijke telefoons. Hierbij benadrukken deze leden dat de uitbreiding van de verplichting om veilig in te loggen naar schatting 1,5 miljoen medewerkers in de zorg zal raken, ten opzichte van de ca. 90.000 die momenteel gebruik maken van een UZI-pas. Met welke zekerheid kan de regering zeggen dat alle 1,5 miljoen medewerkers over een zakelijke telefoon (zullen) beschikken zodra de wet van kracht gaat? Kan worden ingeschat of berekend welk aandeel van deze medewerkers momenteel niet over een zakelijke telefoon beschikt? Genoemde leden doen een beroep op de regering om in goed overleg met verschillende zorgdomeinen dit risico nader uit te werken en te bezien hoe het gebruik van zakelijke telefoons zo veel mogelijk gefaciliteerd kan worden.

De leden van de GroenLinks-PvdA-fractie zijn eveneens bezorgd over de randgevallen met betrekking tot zakelijk telefoongebruik in de zorg. Zij denken bijvoorbeeld aan medewerkers met meerdere werkgevers, waarvan mogelijk verwacht wordt dat zij meerdere werktelefoons tot hun beschikking krijgen. Deze leden vragen daarom aan de regering om samen met zorgmedewerkers en – werkgevers heldere richtlijnen op te stellen voor het gebruiken van zakelijke telefoons. Hierin moet ook duidelijk worden hoe werkgevers verwacht worden te voldoen aan de verwachting dat zij alle relevante medewerkers zullen voorzien van een zakelijke telefoon. Ook zijn genoemde leden benieuwd of, en zo ja hoe, de verwachting dat zorgaanbieders zakelijke telefoons ter beschikking stellen zijn meegerekend in de verwachte uitvoeringskosten van dit wetsvoorstel. Is hiervoor een impactanalyse opgesteld? Zo nee, is de regering bereid om alsnog een impactanalyse uit te voeren in samenwerking met de zorgaanbieders? Hierbij vragen zij tevens om expliciet stil te staan bij het gebruiken van een zakelijke telefoon door zzp'ers in de zorg.

De leden van de GroenLinks-PvdA-fractie hebben bovendien nog vragen over het beheer van zakelijke- en privételefoons om te kunnen voldoen aan het wetsvoorstel. Zij schetsen de situatie waarin een zorgmedewerker een privéwallet, gekoppeld aan de eigen EU Digital Identity Wallet bijvoorbeeld, gebruikt op de zakelijke telefoon. Als deze telefoon in beheer is van de werkgever, treden er dan geen privacyrisico's op? Deze leden vragen om nader toe te lichten hoe de privacy van zorgmedewerkers die een privéwallet gebruiken om zich te identificeren wordt gewaarborgd op zakelijke telefoons. Zij wijzen op het maken van aanvullende afspraken,

die zien op het gebruik van privé en zakelijke telefoons, met de zorgsector als mogelijke oplossing.

De leden van de GroenLinks-PvdA-fractie wijzen erop dat DigiD voor bepaalde zorghandelingen niet geschikt is. Zorgspecifieke inlogmiddelen, bijvoorbeeld voor het digitaal tekenen van recepten, worden door Qualified Trust Service Partners (QTSP's) gedaan. Genoemde leden vragen of de jaarlijkse kosten die worden gemaakt door een QTSP gelijk, of hoger, kunnen uitvallen dan de kosten voor een UZI-pas. Zo lezen deze leden in de beantwoording op hun vragen dat er een stimuleringsregeling van twee jaar wordt voorzien door de overheid om aanschafkosten van nieuwe inlogmiddelen te verlichten. Ten eerste vragen zij om hoe veel geld dit gaat, gezien de veel grotere scope dan het gebruik van UZI-passen. Ten tweede vragen zij of er na die periode van twee jaar structurele compensatie wordt verzorgd. Ten derde vragen zij hoe de regering de rol van marktwerking voor zich ziet om kosten verder te drukken, in relatie tot de kosten voor compliance van QTSP's.

Overheid

De leden van de GroenLinks-PvdA-fractie hebben vragen over de gebruiksvriendelijkheid van de nieuwe werkprocessen. De UZI-pas kent problemen met toegankelijkheid, waardoor het niet makkelijk te gebruiken is in alle werkprocessen. Deze leden krijgen signalen dat QTSP's voornamelijk met nieuwe insteekpassen zullen komen. Daarom vragen zij de regering hoe voorkomen gaat worden dat de nieuwe zorgspecifieke inlogmiddelen niet dezelfde gebruiksproblemen krijgt als de UZI-pas. Welke problemen ziet de regering met de gebruiksvriendelijkheid van de UZI-pas en hoe gaat de regering deze specifiek wegnemen?

Burgers

De leden van de GroenLinks-PvdA-fractie hechten grote waarde aan het inzagerecht van patiënten in hun gegevens. In de beantwoording wordt aangegeven dat onderzocht wordt of de EHDS-verordening aanvullende mogelijkheden biedt om burgers meer regie te geven op hun recht op inzage. Daarover vragen deze leden wat de doel en de scope van het onderzoek is, en welke ideeën de regering zelf heeft op het versterken van het inzagerecht.

Werkbare invoering in de praktijk

De leden van de GroenLinks-PvdA-fractie steunen het doel van een lagere administratieve werkdruk in de zorg van harte. Echter hebben zij vragen over de ervaringen die zijn opgedaan met praktijkproeven, waaronder met het gebruiken van DigiD in het kader van het Nationaal Contactpunt voor eHealth (NCPeH). Deze leden bereiken signalen dat hier uit voort kwam dat medewerkers zich voor elke patiënt opnieuw moesten authentiseren, in plaats van dat dit dagelijks gebeurt zoals geschetst in antwoord op vragen van deze fractieleden onder onderdeel 2.2. Genoemde leden vragen de regering te bevestigen dat zorgmedewerkers zich inderdaad slechts één keer per dagen hoeven te authentiseren via DigiD. Als dit niet waar blijkt, vragen deze leden om te onderbouwen dat er bij een nieuwe authenticatie voor iedere patiënt die wordt behandeld inderdaad sprake is van een significante verminderen van administratieve lasten.

De leden van de GroenLinks-PvdA-fractie hebben dezelfde vraag over het zetten van een digitale handtekening, bijvoorbeeld voor recepten en consulten. Dit zijn handelingen die doorgaans meerdere keren per dag worden uitgevoerd. Zij vragen dan ook hoe er wordt voorkomen dat er

een forse toename van administratieve lasten plaatsvindt voor handelingen die door de dag heen vaker worden uitgevoerd.

De leden van de GroenLinks-PvdA-fractie vinden de regering te weinig concreet over de implementatie op de BES-eilanden. Genoemde leden benadrukken dat het doel moet zijn om een gelijkwaardige bescherming van persoons- en patiëntgegevens te bereiken in heel het Koninkrijk. Daarom vragen zij om nader toe te lichten welke verkenning voor de implementatie op de BES-eilanden er nu plaatsvindt. Op welke termijn is deze afgerond en wat gaat de regering doen als blijkt dat er aanvullende maatregelen nodig zijn om het Dezi-stelsel op de BES-eilanden in te voeren? Vraagt dit mogelijk aanpassingen van dit wetsvoorstel?

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie danken de regering voor de antwoorden op de gestelde vragen in de nota naar aanleiding van het verslag en hebben met interesse kennisgenomen van de beide nota's van wijzigingen. Deze leden maken van de gelegenheid gebruik om nog enkele vragen te stellen. Over de tweede nota van wijziging hebben deze leden geen vragen.

Nota naar aanleiding van het verslag

De leden van de CDA-fractie hebben nog enkele vragen over het belang van strategische autonomie en de nationale veiligheid en de mate van keuzevrijheid bij het gebruik van inlogmiddelen. Deze leden lezen dat dit wetsvoorstel geen mogelijkheid biedt om nadere eisen te stellen op het gebied van strategische autonomie en de nationale veiligheid, en dat dit al geregeld is via het Europese en nationale toezicht. Deze leden begrijpen dat dit waarborgen biedt, maar vragen of dit voldoende is, zeker gezien de actuele (geopolitieke) ontwikkelingen. Genoemde leden vragen of de regering deelt dat de actuele ontwikkelingen, ook de ontwikkelingen rondom de overname van DigiD, laten zien dat het cruciaal is dat we controle hebben over onze eigen IT-infrastructuur, zeker in de zorg. Deze leden vragen of de regering het verstandig acht dat er tenminste één of enkele inlogmiddelen zijn die volledig in Europese handen zijn, en waarvan de regering het gebruik kan stimuleren. Zo ja, dan vragen deze leden hoe de regering hieraan wil werken.

De leden van de CDA-fractie hebben vragen gesteld over de mate van keuzevrijheid die het wetsvoorstel biedt als het gaat om de keuze voor inlogmiddelen. Zij lezen dat de regering beperking van het aantal inlogmiddelen niet vindt passen bij het karakter van een open markt en het belang van innovatie. Genoemde leden vragen of de regering kan aangeven waarom bij een inlogmiddel als DigiD dan wel is gekozen voor één middel en bij eHerkenning voor een aantal erkende leveranciers, terwijl de zorg net zo goed van groot publiek belang is. Deze leden vragen of de regering heeft overwogen om een aantal erkende leveranciers aan te wijzen, zodat de veiligheid en betrouwbaarheid goed geborgd is en voorkomen wordt dat een wildgroei aan inlogmiddelen ontstaat.

Nota van wijziging: Onderdelen G en H

De leden van de CDA-fractie vragen waarom de gefaseerde inwerkingtreding aangepast is, zodat enkele onderdelen in werking treden op 1 januari 2031. Deze leden constateren dat het hiermee nog vijf jaar duurt voordat het verplicht wordt om goedgekeurde inlogmiddelen te gebruiken, en vragen wat eerst de voorgenomen datum was. Genoemde leden vragen ook of het niet verstandiger is deze datum naar voren te

halen, zodat sneller kan worden geborgd dat in de hele zorg gebruik wordt gemaakt van goedgekeurde inlogmiddelen.

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van de Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg. Deze leden hebben hierover de volgende vragen aan de regering.

De leden van de BBB-fractie waarderen het belang van veilige toegang tot cliëntgegevens, maar constateren dat het wetsvoorstel zeer ingrijpende verplichtingen oplegt aan zorgaanbieders, grote administratieve veranderingen met zich meebrengt en forse kosten en technische randvoorwaarden neerlegt bij een sector die al onder grote druk staat.

Genoemde leden constateren dat het wetsvoorstel uitgaat van een verplicht centraal Dezi-register, waarin naar verwachting meer dan 1,5 miljoen zorgmedewerkers moeten worden opgenomen. Ook worden uitsluitend digitale inlogmiddelen met het hoogste betrouwbaarheidsniveau verplicht gesteld. De leden vragen in hoeverre de gevolgen voor kleine zorgaanbieders, zoals zelfstandige praktijken, wijkzorgteams en kleinschalige jeugdhulpaanbieders, realistisch zijn ingeschat. Welke uitvoeringsproblemen verwacht de regering specifiek bij kleinere zorgaanbieders, en welke ondersteuning komt beschikbaar om deze verplichtingen haalbaar te maken? Kan inzichtelijk worden gemaakt welke eenmalige en structurele kosten kleine zorgaanbieders moeten maken om aan dit systeem te voldoen? Hoe voorkomt de regering dat aanbieders afhaken of stoppen omdat deze ICT-verplichtingen voor hen niet uitvoerbaar of betaalbaar zijn?

De leden van de BBB-fractie constateren dat het wetsvoorstel een gefaseerde verplichtstelling kent, maar dat nota's van wijziging meerdere keren de overgangsdata wijzigen, wat leidt tot onduidelijkheid. Genoemde leden vragen waarom het overgangsrecht zo vaak aangepast moet worden en of dit duidt op onvoldoende voorbereiding of technische problemen. Wat verklaart dat binnen één jaar meerdere malen de einddatum van de overgangsperiode moest worden gecorrigeerd? Kan de regering garanderen dat de sector tijdig beschikt over voldoende goedgekeurde inlogmiddelen voordat verplichtingen ingaan? Hoe wordt voorkomen dat zorgaanbieders halverwege moeten overstappen omdat eerdere planning onrealistisch bleek?

De leden van de BBB-fractie constateren dat het wetsvoorstel sterk leunt op technische inlogmiddelen die nog niet bestaan of nog in ontwikkeling zijn. Daarmee wordt de sector verplicht om zich aan te passen aan toekomstige ICT-oplossingen zonder vooraf inzicht in beschikbaarheid, kosten, gebruiksvriendelijkheid of interoperabiliteit. Is de regering bereid een risicoanalyse te delen over het scenario waarin goedgekeurde inlogmiddelen niet tijdig beschikbaar zijn? Hoe beoordeelt de regering de afhankelijkheid van commerciële leveranciers en certificerende instanties bij de uitvoering van een wettelijke verplichting? Waarom is niet gekozen voor een publieke oplossing die garant staat voor continuïteit, in plaats van afhankelijkheid van marktpartijen?

Tot slot merken de leden van de BBB-fractie op dat het wetsvoorstel gepaard gaat met een verplichting voor uitsluitend digitale communicatie met het register. Genoemde leden vragen of dit proportioneel is voor grote aantallen kleinere zorgaanbieders, zeker in regio's waar digitale infrastructuur of digitale vaardigheden beperkt zijn. Hoe beoordeelt de

regering de uitvoerbaarheid voor zorgaanbieders in krimpregio's, waar digitale aansluiting problematischer is en digitale systemen vaker falen? Is de regering bereid uitzonderingen te overwegen voor partijen met beperkte ICT-capaciteit?

Vragen en opmerkingen van de leden van de SGP-fractie

De leden van de SGP-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en van de nota naar aanleiding van het verslag. Zij hebben hierover op dit moment nog een enkele vraag.

Nota naar aanleiding van het verslag: 2.3 Identificatie en authenticatie voor toegang tot cliëntgegevens

De leden van de SGP-fractie sluiten zich aan bij de vragen van de leden van de GroenLinks-PvdA-fractie over het risico dat continuïteit in de zorg afhankelijk wordt van niet-Europese IT-bedrijven. Zij lezen in de beantwoording dat er alleen gebruik zal worden gemaakt van door Nederland erkende en/of onder Europees toezicht staande inlogmiddelen, zodat de continuïteit in de zorg in geen enkel geval volledig afhankelijk wordt van niet-Europese Tech leveranciers. De leden van de SGP-fractie vragen de regering of het niet wenselijker is om vanuit het perspectief van strategische autonomie regelgeving op dit punt aan te scherpen zodat alleen gebruik kan worden gemaakt van software van bedrijven die daadwerkelijk in Nederland of in Europa gevestigd zijn. Zij vragen de regering hierop te reflecteren, waarbij in ieder geval ingegaan wordt op de juridische mogelijkheden hiertoe.

Kan de regering aangeven in hoeverre we ten aanzien van inlogmiddelen op dit moment afhankelijk zijn van niet-Europese marktpartijen? In bredere zin vragen de leden van de SGP-fractie of er door de regering gewerkt aan het in kaart brengen van de afhankelijkheid van niet-Europese bedrijven als het gaat om kritieke functies in de zorg?

De fungerend voorzitter van de commissie,
Mohandis

Adjunct-griffier van de commissie,
Sjerp