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

NOTA NAAR AANLEIDING VAN HET VERSLAG

Inhoudsopgave **blz.**

Introductie

Met belangstelling heb ik kennisgenomen van het nader verslag van de vaste commissie voor Volksgezondheid, Welzijn en Sport van de Tweede Kamer over het voorstel houdende Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg. Er zijn door de leden van de fracties van D66, de VVD, GroenLinks-PvdA, CDA, BBB en de SGP vragen gesteld en opmerkingen gemaakt. Ik hoop met de beantwoording van de gestelde vragen de nog bestaande onduidelijkheden te kunnen wegnemen.

Graag ga ik in op de door de leden van deze fracties gestelde vragen en opmerkingen overeenkomstig de in het nader verslag gekozen paragraafindeling. In deze nota naar aanleiding van het nader verslag zijn de vragen uit het nader verslag opgenomen in cursieve tekst en de beantwoording daarvan in gewone typografie.

Vragen en opmerkingen van de leden van de D66-fractie

1.

*Deze leden van de **D66-fractie** geven aan in de memorie van toelichting vooral te lezen over 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. Deze leden onderschrijven het belang hiervan, maar vragen of ook een expliciete inschatting is gemaakt van mogelijke obstakels voor patiënten en professionals in het zorg- en jeugdveld.*

Het wetsvoorstel heeft geen veranderingen of obstakels op voor patiënten in het zorg- en jeugdveld. Het wetsvoorstel ziet met name op identificatie en authenticatie van zorg- en jeugdhulpmedewerkers die werken bij zorg- en jeugdhulpaanbieders.[1]

Het wetsvoorstel is ontwikkeld in samenwerking met zorgaanbieders en ook zorgprofessionals. Voor wat betreft de zorg- en jeugdhulpmedewerkers geldt dat pilots op verschillende zorgprocessen, onder andere in de ambulance, worden gedaan. Deze pilots hebben tot doel eventuele obstakels vroegtijdig te signaleren, zodat deze voor de daadwerkelijke overgang naar het Dezi-stelsel kunnen worden aangepakt.

Tot nu toe zijn vier pilots uitgevoerd met deelnemers uit de eerstelijnszorg, de ziekenhuissector en de ambulancezorg. Daarbij is gebruikgemaakt van verschillende inlogmiddelen, waaronder DigiD, een wallet en de UZI-pas. Tot dusver kwamen hierbij twee aandachtspunten naar voren. Als eerst kwam naar voren dat de geldigheidsduur van verklaringen invloed kan hebben op de continuïteit van toegang voor zorgmedewerkers. Daarnaast bleek dat zorgmedewerkers moeten wennen aan alternatieve (digitale) inlogmiddelen.

Deze aandachtspunten worden meegenomen in de verdere implementatie van het stelsel.

[1] Het wetsvoorstel ziet op zorgaanbieders, indicatieorganen, zorgverzekeraars en medewerkers en daarnaast jeugdhulpaanbieders, jeugdhulpverleners en medewerkers. Medewerkers zijn natuurlijke personen die werkzaamheden verrichten of gaan verrichten voor zorgaanbieders, jeugdhulpaanbieders, indicatieorganen en zorgverzekeraars en jeugdhulpverleners zijn natuurlijke personen die werkzaamheden verrichten of gaan verrichten voor jeugdhulpaanbieders. Om de terminologie beknopt en helder te houden, wordt in dit nader verslag in het vervolg gesproken over zorg- en jeugdhulpmedewerkers en zorg- en jeugdhulpaanbieders.

2.

*De leden van de **D66-fractie** vragen hoe zorg- en jeugdhulpaanbieders en hun medewerkers praktisch worden ondersteund om mogelijke obstakels bij hen weg te nemen. Daarbij vragen deze leden welke waarborgen er zijn om eventuele opstartproblemen tijdig te signaleren en te verhelpen zodat patiënten en professionals hier geen nadelige gevolgen van ondervinden.*

Het uitgangspunt is dat eventuele opstartproblemen en knelpunten vroegtijdig worden gesignaleerd door middel van genoemde pilots en met monitoring van de implementatie tijdens de overgangsperiode. Daarnaast vindt afstemming plaats met koepelorganisaties en zorg- en jeugdhulpaanbieders. Op die manier kan gericht ondersteuning plaatsvinden, bijvoorbeeld op het gebied van informatievoorziening.

Om zorg- en jeugdhulpaanbieders en hun medewerkers te ondersteunen, zet ik in op praktische ondersteuning zoals het instellen van een servicedesk en het informeren via verschillende kanalen en handreikingen. Via de servicedesk kunnen concrete vragen gericht worden beantwoord. Via de overige communicatie, waaronder de handreikingen, wordt meer algemene informatie verstrekt over wat je bijvoorbeeld als zorg- en jeugdhulpaanbieders en zorg- en jeugdhulpmedewerker moet doen om aan te kunnen sluiten op het Dezi-stelsel of om in te schrijven in het Dezi-register. De resultaten uit de eerdergenoemde pilots worden ook opgenomen in de handreiking.

3.

*De leden van de **D66-fractie** constateren dat het vereiste betrouwbaarheidsniveau hoog veel veiligheidsrisico's afdekt. Zij vragen of de regering echter specifiek kan aangeven welke risico's resteren na implementatie van dit niveau.*

Het wetsvoorstel ziet toe op een deel van de informatiebeveiliging, namelijk uitsluitend de identificatie en authenticatie van zorg- en jeugdhulpmedewerkers en zorg- en jeugdhulpaanbieders. Hoewel het vereiste betrouwbaarheidsniveau hoog hiermee veel risico's ondervangt, dekt het niet alle risico's op het gebied van de verwerking van gezondheidsgegevens af. Zo zullen met inzet van al deze maatregelen alsnog risico's blijven voortbestaan die buiten de reikwijdte van het wetsvoorstel vallen, zoals: menselijke fouten bij de toewijzing van autorisaties, het uitlenen van inlogmiddelen en technische en fysieke kwetsbaarheden die zich buiten het Dezi-stelsel voordoen. Voor deze resterende risico's moeten zorg- en jeugdhulpaanbieders hun verantwoordelijkheid nemen en maatregelen treffen die noodzakelijk zijn om tot een juiste informatiebeveiliging van medische gegevens te komen.[2]

4.

*De leden van de **D66-fractie** vragen wie de verantwoordelijkheid draagt wanneer de risico's die resteren na implementatie van het betrouwbaarheidsniveau hoog zich materialiseren: de overheid (als stelselverantwoordelijke), de leverancier van het inlogmiddel, of de individuele zorgaanbieder?*

De vraag voor wiens verantwoordelijkheid een risico komt, is niet in algemene zin te beantwoorden. Dat ligt immers altijd aan de concrete omstandigheden van het geval.

[2] Zoals de NEN 7510 (het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg), de NEN 7512 (nadere uitwerking van de NEN 7510 betreffende de veiligheid van de gegevensuitwisseling tussen partijen in de zorg) en de NEN 7513 (de norm voor het gestructureerd vastleggen van acties op elektronische patiëntendossiers in de zorg).

Voor wat betreft de verantwoordelijkheden uit het wetsvoorstel geldt in elk geval dat ik verantwoordelijk ben voor: de inrichting en het beheer van het register (artikel 14 en 7.2.7 van het wetsvoorstel), de goedkeuring van een inlogmiddel en de koppeling van een inlogmiddel aan een in het register geregistreerde, alsmede voor het verlenen, weigeren, schorsen of intrekken van goedkeuring (artikelen 14a en 7.2.7 wetsvoorstel). Voor zorg- en jeugdhulpaanbieders liggen verantwoordelijkheden voor wat betreft de betaling van een vergoeding (artikelen 14 en 7.2.7 van het wetsvoorstel), de inschrijving in het register, het voorzien in de mogelijkheid tot en het gebruik van verschillende inlogmiddelen (artikelen 15 en 7.2.8 van het wetsvoorstel). Het wetsvoorstel legt geen verantwoordelijkheden bij leveranciers van inlogmiddelen.

Hierbij zij benadrukt dat de verplichtingen uit overige wet- en regelgeving, zoals het treffen van passende technische en organisatorische maatregelen, onverkort gelden.[3]

5.

*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. Zij vragen hoe wordt voorkomen dat een inlogmiddel op betrouwbaarheidsniveau hoog toch onveilig wordt door malware op een slecht onderhouden privételefoon.*

De eisen aan inlogmiddelen op betrouwbaarheidsniveau hoog zijn zo gesteld dat een inlogmiddel op een telefoon weerstand moet bieden tegen aanvallen met een hoog aanvalspotentieel en daarmee tegen malware (ongewenst kwaadaardige software).

Dit kan worden bereikt door middel van (technische) maatregelen die beveiliging op verschillende lagen regelt en waarmee (bijvoorbeeld) malware kan worden gedetecteerd en zo het inlogmiddel onbruikbaar maken.

Een zeer belangrijke beveiligingsmaatregel die in de praktijk vaak wordt toegepast is dat het geheime sleutelmateriaal van het inlogmiddel niet in het (gewone) geheugen van de telefoon wordt geplaatst. Moderne telefoons hebben namelijk een beveiligd deel: het *Secure Element*. Dit deel werkt als digitale kluis die losstaat van de rest van het toestel en waar het besturingssysteem zelf niet direct bij kan. Zelfs als er malware op de telefoon staat, kan de malware geen toegang krijgen tot de sleutels die in het Secure Element zijn opgeslagen.

Tenslotte vereist de eIDAS-verordening voor betrouwbaarheidsniveau hoog dat er sprake moet zijn van dynamische authenticatie.[4] Dit betekent dat iedere keer dat wordt ingelogd op de telefoon er een uniek bewijs wordt gemaakt dat bij iedere inlog anders is.

Het gebruik van een inlogmiddel dat niet meer betrouwbaar is, is absoluut onwenselijk. De aanbieders van deze middelen moeten daartoe dus de maatregelen treffen om te voldoen aan de eisen voor betrouwbaarheidsniveau hoog, en zo te voorkomen dat een inlogmiddel dat niet meer betrouwbaar is, gebruikt kan worden in het geval een persoonlijk apparaat niet goed wordt onderhouden.

---

[3] Artikel 32 van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens
en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).

[4] Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt(*PbEU* 2015, L 235/7), bijlage artikel 1, onderdeel 3.

6.

*De leden van de **D66-fractie** vragen daarbij of het inlogmiddel in staat is om te detecteren of een apparaat gehackt is, door bijvoorbeeld spionagesoftware, alvorens toegang ertoe verleend kan worden.*

Besturingssystemen van telefoons kunnen manieren bieden om te detecteren of het besturingssysteem zelf en de applicaties daarop integer zijn. Leveranciers van middelen op betrouwbaarheidsniveau hoog zullen gezien de hoge eisen aan de inlogmiddelen doorgaans gebruik maken van dit soort technologie.

Hoewel deze detectietechnieken veilig zijn, zijn ze niet onfeilbaar en bovendien staan de ontwikkelingen (bijvoorbeeld door nieuwe kwetsbaarheden die bekend worden) niet stil. Het is daarom vereist dat beveiliging steeds meegroeit met nieuwe uitvindingen en dreigingen. Om die reden is de eIDAS-verordening technologieneutraal opgesteld en verplicht de verordening verleners van vertrouwensdiensten via passende technische en organisatorische maatregelen de risico's te beheren in verband met de veiligheid van de door hen verleende vertrouwensdiensten.[5] Deze maatregelen waarborgen, rekening houdend met de meest recente technologische ontwikkelingen, een veiligheidsniveau dat in verhouding staat tot de mate van risico.

7.

*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. De leden van de D66-fractie vragen of de regering kan concretiseren hoe vaak audits zullen plaatsvinden.*

Bij de NEN 7518 hoort ook een certificatieschema: het NCS 7518. Dit certificatieschema beschrijft de eisen voor instellingen die inspecties ten behoeve van de uitgifte van zorgspecifieke inlogmiddelen in de zorg uitvoeren. Er is op dit moment nog sprake van een concept-certificatieschema, omdat de relevante NEN-norm nog niet is aangenomen. Naast een initiële beoordeling voorziet dit schema ook in opvolgende periodieke beoordelingen. Op dit moment wordt in het concept-schema voorzien in een certificering die maximaal 3 jaar geldig zal zijn, met een jaarlijks verplichte surveillance-audit waarin verschillende onderdelen gecontroleerd zullen worden.

8.

*De leden van de **D66-fractie** vragen of de regering een periodieke audit voldoende acht, of dat er ook sprake is van continu toezicht of steekproeven.*

Er wordt in het concept-certificatieschema van de NEN 7518 voorzien in het gebruik van steekproeven als een verplicht onderdeel van de surveillance-audit. Naast deze audit worden ook andere vormen van toezicht voorzien. Zo staan de zorg- en jeugdhulpaanbieders onder toezicht van de IGJ en onder toezicht van de certificerende instantie van de NEN 7518.[6] Een zorg- en jeugdhulpaanbieder is verplicht veranderingen onverwijld te melden aan de certificerende instantie, waarna deze de veranderingen beoordeelt en besluit over de gevolgen voor de certificatie. De middelenleverancier staat vanuit zijn rol als *Qualified Trust Service Provider* (QTSP) onder toezicht

[5] Overwegingen 16 en 27 van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU2014,* L257/73).

[6] Artikel I, onderdeel C, Wetsvoorstel DIAZ.

van Rijkinspectie Digitale Infrastructuur, het nationale toezichtsorgaan onder de Verordening.[7] Op grond van de Verordening is de rijksinspectie bevoegd om op te treden, bijvoorbeeld door aanvullende audits uit te (laten) voeren bij de middelenleverancier.

9.

*De leden van de **D66-fractie** willen weten hoe technisch en procedureel gegarandeerd wordt dat het BSN daadwerkelijk direct en onherstelbaar uit de administratie van de middelenuitgever wordt verwijderd na de koppeling met het Dezi-nummer.*

Via de NCS 7518 worden eisen gesteld ten aanzien van het registratie- en het uitgifteproces van de zorgspecifieke middelen. De (technische) inrichting van systemen, waardoor het BSN na de omwisseling tot een Dezi-nummer niet meer voor dit doeleinde beschikbaar is, is onderdeel van de opgenomen eisen. De middelenuitgever moet hier aan blijven voldoen.

10.

*De leden van de **D66-fractie** zijn daarbij ook benieuwd welke gevolgen er in werking treden bij het niet naleven van deze verwijderplicht.*

Het niet naleven van de verwijderplicht heeft gevolgen voor de certificering van het zorgspecifieke middel. Als het zorgspecifieke middel niet langer voldoet aan de NEN 7518, kan dat een reden vormen om de goedkeuring van het inlogmiddel te schorsen of in te trekken, wat betekent dat het middel niet langer gebruikt kan worden in het Dezi-stelsel.

Voorts kan het niet naleven van de verwijderplicht tevens een overtreding opleveren van de Algemene Verordening Gegevensbescherming (hierna: AVG). In dat geval is de Autoriteit Persoonsgegevens bevoegd om op te treden.

11.

*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. Deze leden willen weten wat er concreet in deze afspraken staan.*

Het huidige hostingcontract is gesloten op basis van de Algemene rijksvoorwaarden bij IT overeenkomsten 2018 (ARBIT-2018).[8] Een exit-clause en afspraken over de te nemen stappen bij ontbinding zijn hier een vast onderdeel van. In aanvulling zijn er specifieke contractuele bepalingen opgenomen over geheimhouding, het gebruik van data en de wijze en termijn van terug levering van data.

12.

[7] Artikel 17 van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU2014,* L257/73). Een QTSP, ook wel een gekwalificeerde verlener van vertrouwensdiensten genoemd, is een verlener van vertrouwensdiensten die een of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen, zie: artikel 3, onderdeel, 20 van de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU2014,* L257/73).

[8] Besluit vaststelling Algemene Rijksvoorwaarden voor inkoop (ARBIT-2018, ARIV-2018 en ARVODI-2018) (Stcrt. 2018/26414).

*De leden van de **D66-fractie** vragen 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.*
In het huidige hostingcontract zijn boeteclausules opgenomen die moeten voorkomen dat de leverancier in gebreke blijft. Ook worden er aanvullend continuïteitsplannen opgesteld. Dit wordt periodiek getest. Daarnaast is de software door de overheid zelf ontwikkeld, wat eventuele overgang naar een andere leverancier vergemakkelijkt.

13.

*De leden van de **D66-fractie** geven aan dat in de nota naar aanleiding van het verslag wordt geantwoord dat het Nederlands recht van toepassing is op het Dezi-register. Hierop voortbordurend vragen de leden van de D66-fractie of er voldoende is gewaarborgd dat deze data bij eventuele overnames door buitenlandse bedrijven nooit buiten de EU bewaard, ingezien of gebruikt kan worden.*

Contractueel zijn er afspraken gemaakt over de locatie van de data en de bescherming ervan. Via een preferente aandelenconstructie is de leverancier beschermd tegen vijandige overnames, wat moet voorkomen dat de gegevens alsnog buiten de EU bewaard, ingezien of gebruikt kunnen worden. Ook zijn er aanvullende afspraken gemaakt over hoe er gehandeld dient te worden wanneer een niet-Nederlandse overheidsdienst om gegevens verzoekt. Tot slot bevat de ARBIT-2018 de mogelijkheid tot ontbinding indien er sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de leverancier. Bij een ontbinding kan verzocht worden om retournering van de data.

14.

*De leden van de **D66-fractie** vragen hoe de technische en juridische aansluiting van het Dezi-stelsel op de EUDI-wallet exact wordt vormgegeven.*

Voor wat betreft de technische aansluiting moet onderscheid worden gemaakt tussen twee processen. Enerzijds het uitgeven van de verklaring van de zorgidentiteit aan de EU Digital Identity Wallet (hierna: EUDI-wallet) en anderzijds het gebruik van deze verklaring vanuit de wallet voor de toegang tot zorginformatie- en gegevensuitwisselingssystemen.

Bij de uitgifte van de verklaring van de zorgidentiteit fungeert het Ontkoppelpunt van het CIBG, dat zal voldoen aan de Europese eisen, als centrale veilige schakel. In dit proces maakt de zorg- of jeugdhulpmedewerker het BSN bekend aan het Dezi-register, via de in de EUDI-wallet opgeslagen Personal Identification Data (PID). Het Ontkoppelpunt controleert daarbij de relevante zaken, zoals de authenticiteit van de wallet, de Europese erkenning en de koppeling met de gebruiker. Nadat deze controle goed is doorlopen, maakt het Dezi-register een (digitale) verklaring van de zorgidentiteit, die vervolgens wordt aangeboden aan de EUDI-wallet van de zorg- of jeugdhulpmedewerker. Doordat de verklaring is opgesteld volgens de Europese standaarden, kan de zorg- en jeugdhulpmedewerker de zorgidentiteit veilig opslaan in elke erkende EUDI-wallet.

De toegang tot zorginformatie- en uitwisselingssystemen met behulp van de EUDI-wallet kan plaatsvinden door middel van een wallet-koppelvlak dat de zorg- of jeugdhulpaanbieder zelf kan implementeren, of wanneer de zorg- of jeugdhulpaanbieder dit koppelvlak niet heeft door gebruik te maken van een centrale voorziening bij het CIBG. In het eerste geval wordt de digitale zorgidentiteit uit de wallet bij de zorg- of jeugdhulpaanbieder ontvangen en geverifieerd. In het tweede geval fungeert het CIBG als tussenstation: de zorg- of jeugdhulpmedewerker logt met de wallet in bij het CIBG, waarna het CIBG de authenticatieverklaring (de bevestiging) verstrekt in

een technisch formaat dat de zorg- of jeugdhulpaanbieder kan ontvangen. De standaarden, protocollen en formats voor informatie-uitwisseling tussen uitgevers (zoals het CIBG), EUDI-wallets en dienstverleners zijn in het *Architecture and Reference Framework* (ARF) van eIDAS vastgesteld.[9]

Voor wat betreft de juridische aansluiting op EUDI-wallets geldt dat door het Ministerie van Binnenlandse zaken een uitvoeringswet wordt voorbereid. Deze uitvoeringswet strekt tot het beschikbaar stellen van een publieke wallet en tot het normeren van het juridische kader waarbinnen het EUDI-stelsel functioneert. Het wetsvoorstel laat de inlogmiddelen erkend door de Wet digitale overheid (hierna: Wdo) toe, voor zover deze voldoen aan betrouwbaarheidsniveau hoog. Hiermee komt de NL-wallet beschikbaar voor identificatie en authenticatie van de zorg- en jeugdhulpmedewerker, dit is de nationale versie van de EUDI-wallet. Het voornemen is om in 2026 te starten met een Proof-of-Concept met Dezi en de publieke NL Wallet.

15.

*De leden van de **D66-fractie** vragen of de Europese acceptatieplicht betekent dat Nederlandse zorgaanbieders vanaf eind 2026 direct verplicht zijn om ook buitenlandse "wallets" van tijdelijke arbeidskrachten te accepteren, en of de systemen van de Nederlandse zorgaanbieders daarop voorbereid zijn.*

De bedoelde acceptatieplicht voor de zorg- en jeugdhulpaanbieder ziet toe op het verlenen van toegang tot publieke en private diensten.[10] De toegang tot de Sectorale Berichtenvoorziening in de Zorg (SBV-Z) en zorginformatie- en elektronische uitwisselingssystemen is geen publieke of private dienst die de zorg- en jeugdhulpaanbieder aan diens medewerker levert. Er geldt daarom op dat punt geen acceptatieplicht voor buitenlandse "wallets" van tijdelijke arbeidskrachten voor het inloggen op bedoelde systemen.

Bij de toegang tot bedoelde systemen door de zorg- of jeugdhulpmedewerker, treedt de medewerker namelijk niet op als natuurlijke persoon, maar namens en ten behoeve van de zorg- of jeugdhulpaanbieder voor wie de medewerker werkzaamheden verricht. Dit betreft niet een online dienst die door de zorg- of jeugdhulpaanbieder wordt verleend, maar een dienst die wordt verleend door het CIBG (in geval van de toegang tot SBV-Z), binnen de eigen organisatie van de zorg- of jeugdhulpaanbieder (in geval van een zorginformatiesysteem), of bij de toegang tot het elektronisch uitwisselingssysteem, zoals het LSP, door de aanbieder van dat uitwisselingssysteem.
Kortom, nu het geen online dienst is die door de zorg- en jeugdhulpaanbieder aan de buitenlandse medewerker wordt verleend, ontstaat ook geen acceptatieplicht ten aanzien van de buitenlandse wallet voor de toegang tot genoemde systemen.

[9] eIDAS Expert Group, *Architecture and reference framework*, November 2023. De ARF beschrijft de gemeenschappelijke normen, richtsnoeren, technische specificaties en best practises die de lidstaten samen ontwikkelen en die gebruikt worden voor informatie-uitwisseling tussen wallets, uitgevers en dienstverleners in de Europese Unie.

[10] Artikel 5 bis, eerste lid, van de Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit.

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

Inleiding

16

*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. De leden 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.*

In de nota naar aanleiding van het verslag (Kamerstukken II 2025/26, 36 702 nr. 6) is melding gemaakt van een pilot met de EUDI-wallet. In de periode sinds het verzenden van deze nota naar aanleiding van het verslag heb ik dit voorstel nader verkend samen met het programma EDI van het ministerie van BZK.

Een EUDI-wallet is een digitale wallet die uitgegeven of erkend is door een EU-lidstaat en voldoet aan de eisen van de herziene eIDAS-verordening. Het gebruik van een EUDI-wallet is voor de burger of een zorg- en jeugdhulpmedewerker vrijwillig. We beogen een Proof of Concept (PoC) waarin wordt aangetoond dat het Dezi-stelsel werkt met de EUDI-wallet. De publieke NL-wallet gaat worden ingezet binnen de PoC.

In de PoC zullen drie functionaliteiten worden beproefd. In de eerste plaats gaat het om het proces van uitgifte, waarbij een verklaring van de zorgidentiteit wordt gegenereerd en veilig in de wallet wordt geladen. Vervolgens richt de PoC zich op de verificatie van deze identiteit, door aan te tonen dat het mogelijk is om met behulp van de wallet in te loggen bij zowel het Dezi-register als bij systemen, zoals een elektronische patiëntendossiers, van een zorg- of jeugdhulpaanbieder. Tot slot wordt de functionaliteit digitaal ondertekenen getest, waarbij een zorgverlener met behulp van de wallet kan ondertekenen met de eigen zorgidentiteit. De verkenning en uitwerking van de beproevingsmogelijkheden zijn nog niet afgerond.

Het huidige UZI-register en de inlogmiddelen

17

*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.*

Een zeer belangrijke beveiligingsmaatregel is dat het geheime sleutelmateriaal van het inlogmiddel niet in het (gewone) geheugen van de telefoon wordt geplaatst. Moderne telefoons hebben namelijk een beveiligd deel: het *Secure Element*. Dit deel, in de vorm van een chip, werkt als digitale kluis die losstaat van de rest van het toestel. Zelfs als er malware op de telefoon staat, kan de malware geen toegang krijgen tot de sleutels die in het *Secure Element* zijn opgeslagen.

Daarnaast is er de mogelijkheid tot controle op de veiligheid van het toestel. Een inlogmiddel (als applicatie) controleert dan voortdurend of de telefoon nog wel veilig is om te gebruiken. Hiermee wordt gecontroleerd of de telefoon is aangepast (*ge-root* of *ge-jailbreakt* waarbij de beveiliging door de gebruiker zelf is omzeild). Als dat zo is, weigert de applicatie te werken.

Malware probeert vaak mee te kijken op het scherm of de gebruiker naar een vals inlogscherm te lokken. Om dit te voorkomen kunnen applicaties technieken toepassen die voorkomen dat andere applicaties mee kunnen kijken op het scherm of 'over de app heen' kunnen liggen.

Een eis van de eIDAS-verordening is dat inlogmiddelen op een betrouwbaarheidsniveau hoog altijd om een bewuste handeling vragen. Dit is omdat er voor betrouwbaarheidsniveau hoog minimaal twee verschillende authenticatiefactoren, zoals kennis bezit of biometrie) moeten worden toegepast om de authenticatie uit te voeren. Een voorbeeld hiervan is het scannen van een vingerafdruk (biometrie) in combinatie met het invoeren van een pincode (kennis).[11]

Tenslotte is van belang dat betrouwbaarheidsniveau hoog vereist dat er sprake moet zijn van dynamische authenticatie.[12] Dit betekent dat iedere keer dat wordt ingelogd op de telefoon er een uniek bewijs wordt gemaakt dat bij iedere inlog anders is. Dit betekent dat zelfs als de malware onderdelen of signalen van de inlogpoging opvangt, deze niet kunnen worden hergebruikt voor andere toegang.

Hoewel de technieken van nu erg veilig zijn, staat de ontwikkeling niet stil. Het is belangrijk dat beveiliging steeds meegroeit met nieuwe uitvindingen en dreigingen. Om die reden is de eIDAS-verordening, waar vanuit het wetsvoorstel voor het bepalen van betrouwbaarheidsniveaus naar wordt verwezen, technologieneutraal opgesteld. De verordening verplicht verleners van vertrouwensdiensten om via passende technische en organisatorische maatregelen de risico's te beheren in verband met de veiligheid van de door hen verleende vertrouwensdiensten.[13] Deze maatregelen waarborgen, rekening houdend met de meest recente technologische ontwikkelingen, een veiligheidsniveau dat in verhouding staat tot de mate van risico.

18

*De leden van de **GroenLinks-PvdA-fractie** zijn benieuwd of naar aanleiding van dit wetsvoorstel ook meer aandacht gegeven wordt aan het voorkomen van cyberveiligheidsrisico's onder zorgmedewerkers.*

Cyberveiligheid is van ons allemaal, iedereen heeft hierin een rol te pakken. Met het programma 'Informatieveilig gedrag in de zorg' werk ik aan het verhogen van bewustzijn van zorgmedewerkers en het voorkomen van cyberveiligheidsrisico's. In de brief 'Informatiebeveiliging in de zorg' van 4 december 2025 heb ik u hier nader over geïnformeerd.[14] Dit programma loopt sinds 2019 en biedt kosteloos methoden aan om informatieveilig gedrag bij medewerkers in de zorg te stimuleren. Met het programma wordt daarmee ingezet op het verhogen van de digitale weerbaarheid. Dit gebeurt door het verhogen van kennis en bewustzijn waarmee incidenten voorkomen kunnen worden. Een voorbeeld hiervan is het aanbieden van mogelijke interventies om te voorkomen dat zorgmedewerkers slachtoffer worden van *phishing*. Ook biedt het programma methoden om medewerkers te leren wat te doen als het toch misgaat. Het programma biedt bijvoorbeeld praktische tips over het stimuleren van medewerkers om een datalek te melden.
19

[11] Paragraaf 2.1.2 van het Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (*PbEU* 2015, L 235/7).

[12] Paragraaf 2.3.1 van het Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (*PbEU* 2015, L 235/7).

[13] Overwegingen 16 en 27 van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU 2014,* L257/73).

[14] Kamerstukken II, 2025-2026, 27 529 nr. 353.

*De leden van de **GroenLinks-PvdA-fractie** vragen of de regering de mening deelt dat een toename in het gebruik van digitale inlogmiddelen gepaard moet gaan met een brede inzet op de digitale weerbaarheid van zorgmedewerkers.*

Digitale weerbaarheid is een belangrijk onderdeel van onze samenleving en daarmee ook van de zorg. Met dit wetsvoorstel komt de noodzaak voor digitale weerbaarheid meer naar voren. Het volgen van het programma 'Informatieveilig gedrag in de zorg' wordt daarom benadrukt. Daarnaast is er volop ondersteuning tijdens de implementatiefase van dit wetsvoorstel, het ondersteunen van zorgmedewerkers en het onderstrepen van digitale weerbaarheid bij hen is daarbij ook een onderdeel van.

20

*De leden van de **GroenLinks-PvdA-fractie** vragen daarbij ook of de regering kan reflecteren op de rol van dit wetsvoorstel om datalekken te voorkomen.*

Een juiste en veilige inrichting van een stelsel van identificatie en authenticatie, zoals voorzien met dit wetsvoorstel, speelt een belangrijke rol bij het voorkomen van datalekken veroorzaakt door onrechtmatige toegang door foutieve identificatie en/of authenticatie. Andere beveiligingsmaatregelen blijven daarnaast onontbeerlijk.

21

*De leden van de **GroenLinks-PvdA-fractie** vragen om in te schatten of, en zo ja hoeveel, cyberincidenten in 2025 voorkomen hadden kunnen worden als dit wetsvoorstel van kracht was geweest.*

Het is niet mogelijk om in te schatten hoeveel cyberincidenten in 2025 voorkomen hadden kunnen worden als het wetsvoorstel van kracht zou zijn geweest. In de eerste plaats worden niet alle cyberincidenten gemeld. Ook is niet altijd duidelijk wat de precieze oorzaak van een incident is geweest. Bovendien zijn de gegevens over het jaar 2025 nog niet door de Autoriteit Persoonsgegevens bekend gemaakt. Zij publiceert de datalekrapportage namelijk jaarlijks in mei/juli over het voorgaande jaar. Uit de jaarrapportage van 2024 blijkt in elk geval dat 42% van de gemelde cyberaanvallen werd veroorzaakt door account-takeovers.[15] Hierbij krijgen kwaadwillenden ongeautoriseerd toegang tot accounts.

Voorts meldt de AP in dezelfde rapportage dat zij bij 253 organisaties heeft onderzocht hoe cybercriminelen toegang kregen tot de systemen. In 12% van de gevallen bleek dit te zijn gelegen in menselijke misleiding, zoals het invoeren van inloggegevens na het klikken op een *phising-link*. Ook bleek dat regelmatig veelgebruikte of eerder gelekte wachtwoorden werden gebruikt om toegang te krijgen (*credential stuffing*).

Account-takeovers, toegang via *phising-links* en *credential stuffing* zijn te voorkomen door het gebruik van goedgekeurde inlogmiddelen op betrouwbaarheidsniveau hoog, zoals verplicht onder het wetsvoorstel DIAZ.

22

*De leden van de **GroenLinks-PvdA-fractie** vragen of de regering de toename van kosten en administratieve lasten proportioneel acht aan de afname aan cyberveiligheidsrisico's in de zorg, als hier inderdaad sprake van is.*

[15] Autoriteit Persoonsgegevens, *Rapportage datalekken 2024,* 3 juli 2025, link: Rapportage datalekken 2024 | Autoriteit Persoonsgegevens.

Het wetsvoorstel voorziet in een juiste en veilige inrichting van een stelsel voor identificatie en authenticatie van zorg- en jeugdhulpmedewerkers. Daarmee wordt een specifiek en afgebakend onderdeel van de informatiebeveiliging versterkt, namelijk het voorkomen van onrechtmatige toegang tot zorgsystemen als gevolg van onvoldoende betrouwbare identificatie en authenticatie.

De regering acht de met het wetsvoorstel gemoeide kosten proportioneel in verhouding tot het te mitigeren cyberveiligheidsrisico. Daarbij is van belang dat zorgsystemen gevoelige en bijzondere persoonsgegevens bevatten en dat de zorgsector in de praktijk regelmatig doelwit is van cyberaanvallen.[16] Incidenten kunnen leiden tot datalekken en verstoringen van primaire zorgprocessen, met directe gevolgen voor patiënten en zorg- en jeugdhulpmedewerkers.

Ten aanzien van de administratieve lasten voor identificatie en authenticatie geldt dat het wetsvoorstel niet uitgaat van een structurele toename. Op korte termijn kan sprake zijn van een implementatie-inspanning bij zorg- en jeugdhulpaanbieders. Daar staat tegenover dat met de invoering van gestandaardiseerde inlogmiddelen op langere termijn een structurele vermindering van administratieve lasten wordt verwacht, onder meer door uniformering van beheerprocessen. De zorg- of jeugdhulpmedewerker heeft de keuze om gebruik te maken van het inlogmiddel dat het beste past bij het zorgproces. Voor zorg- of jeugdhulpmedewerkers met meerdere werkgevers betekent dit bijvoorbeeld dat zij niet voor iedere werkgever een ander inlogmiddel hoeven te gebruiken, maar dat één inlogmiddel volstaat.

Daarbij geldt wel dat de concrete verhouding tussen kosten en afname aan cyberveiligheidsrisico's per zorg- en jeugdhulpaanbieder verschilt. Dit hangt onder meer samen met de omvang van de organisatie en de bestaande ICT-infrastructuur.

Medewerkers registreren in het Dezi-register

23

*De leden van de **GroenLinks-PvdA-fractie** hebben vragen over de formulering van dit onderdeel van het wetsvoorstel. 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.*

Het wetsvoorstel is van toepassing op 'de zorgmedewerker'. Het deel van het wetsvoorstel dat wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) voorstelt, definieert dit begrip als: "zorgverlener in de zin van artikel 1 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz), of eenieder die werkzaamheden verricht of gaat verrichten voor een zorgaanbieder, indicatieorgaan of zorgverzekeraar en daarbij cliëntgegevens verwerkt." Dit brengt met zich mee dat ook ZZP-ers en medewerkers die in een ander dienstverband voor de zorgaanbieder werkzaam zijn onder de reikwijdte van het wetsvoorstel vallen.

Het wetsvoorstel heeft een positieve impact op de ZZP-er in de zorg, nu deze op basis van het voorgestelde artikel 14 kan worden ingeschreven in het Dezi-register en op basis van het voorgestelde artikel 15 met een goedgekeurd inlogmiddel gebruikmaken van elektronische uitwisselingssystemen en zorginformatiesystemen. Het wetsvoorstel biedt dezelfde mogelijkheden ook voor jeugdhulpmedewerkers

[16] Z-Cert, *Cybersecurity Dreigingsbeeld voor de zorg 2024,* link: Cybersecurity Dreigingsbeeld voor de zorg 2024 - Z-CERT.

door voorgestelde artikelen 7.2.7 en 7.2.8 van het wetsvoorstel. Zo kan de ZZP-er gebruikmaken van hetzelfde inlogmiddel bij de verschillende zorg- of jeugdhulpaanbieders voor wie hij werkzaam is. Dit verhoogt niet alleen het gebruiksgemak voor een ZZP'er qua werkzaamheden, maar zorgt er ook voor dat de ZZP-er snel ingezet kan worden. Er bestaat immers al een registratie van deze ZZP-er.

24

*De leden van de **GroenLinks-PvdA-fractie** hebben aanvullende vragen over de uitgifte van de nieuwe inlogmiddelen. In de beantwoording in de nota naar aanleiding van het verslag 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.*

Het aanvragen van, in dit geval een zorgspecifieke inlogmiddel, kost niet één tot twee dagen. De duur van één of twee dagen waarnaar verwezen wordt, gaat over het uitvoeren van een audit om te komen tot een certificaat van conformiteit met de NEN 7518. Deze één tot twee dagen is de inschatting van experts.

Alvorens zorgspecifieke middelen op basis van de NEN 7518 te mogen uitgeven, moet een zorg- of jeugdhulpaanbieder een NEN 7518 certificaat verkrijgen. Dit certificaat van conformiteit toont aan dat de gecertificeerde zorgspecifieke middelen voldoen aan de eisen van de NEN518. Dit staat los van het (vervolgens) daadwerkelijk uitgeven van deze inlogmiddelen aan zorg- en jeugdhulpmedewerkers.

Voor wat betreft de terugvalopties of tijdelijke middelen bij acute inhuur geldt dat de medewerkers bij een zorg- of jeugdhulpaanbieder op basis van het voorgestelde artikel 15 en 7.2.8 van het wetsvoorstel alle goedgekeurde middelen kunnen gebruiken voor toegang tot de SBV-Z en van elektronische uitwisselingssystemen of zorginformatiesystemen. Hiermee zijn de terugvalopties en tijdelijke middelen reeds gegeven. De zorg- of jeugdhulpmedewerker kan immers ook gebruik maken van de beschikbare publieke middelen van de Wdo en (zodra beschikbaar) de publieke NL-wallet. Zodra de zorg- of jeugdhulpaanbieder de werkrelatie met de medewerker kenbaar maakt, kan het inlogmiddel binnen enkele minuten door de zorg- of jeugdhulpmedewerker worden gebruikt.

25

*De leden van de **GroenLinks-PvdA-fractie** vragen welke risico's de regering ziet dat zulke casussen voorkomen.*

De regering ziet het risico dat zorg- of jeugdhulpmedewerkers bij acute inhuur geen tijdige toegang tot zorgsystemen krijgen als zeer beperkt.

De zorg- of jeugdhulpaanbieder moet op basis van artikel 15 en artikel 7.2.8 van het wetsvoorstel immers alle goedgekeurde middelen accepteren. De zorg- of jeugdhulpmedewerker kan daardoor ook gebruik maken van de beschikbare publieke middelen, zoals de publieke NL-wallet (zodra beschikbaar) en de Wdo, dit nadat de zorg- of jeugdhulpaanbieder de werkrelatie met de medewerker kenbaar heeft gemaakt.

26

*De leden van de **GroenLinks-PvdA-fractie** vragen daarbij of dit in de risico-inventarisatie is meegenomen.*

Bij het inventariseren van de risico's van de opzet van het Dezi-stelsel is aandacht besteed aan de vraag hoe om te gaan met de benodigde eigenschappen en functionaliteit van de inlogmiddelen om uitval of onbruikbaarheid in zorgprocessen te voorkomen en ruimte te bieden aan specifieke eisen (bijvoorbeeld hygiëne) vanuit het zorgveld. Daarbij is rekening gehouden met de beperkingen van het bestaande UZI-middel, waarin het ontbreken van flexibiliteit en terugvalopties als knelpunt werden ervaren en ook duidelijk was dat inzet in ambulante omgevingen in toenemende mate cruciaal is en tegelijkertijd problematisch.[17]

Juist om deze risico's te mitigeren, is bij de opzet van het Dezi-stelsel gekozen voor een stelsel waarin meerdere inlogmiddelen zijn toegestaan en zorg- en jeugdhulpaanbieders op grond van artikelen 15 en 7.2.8 van het wetsvoorstel verplicht zijn alle goedgekeurde inlogmiddelen te accepteren. De beschikbaarheid van publieke inlogmiddelen onder de Wdo en de eIDAS-verordening kunnen daarbij als terugvaloptie dienen.

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

27

*De leden van de **GroenLinks-PvdA-fractie** geven aan een cyberveiligheidsrisico door zorgdomeinen te zien 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. De leden van de Groenlinks-PvdA-fractie vragen met welke zekerheid de regering kan zeggen dat alle 1,5 miljoen medewerkers over een zakelijke telefoon (zullen) beschikken zodra de wet van kracht gaat.*

Het wetsvoorstel introduceert geen verplichting tot het gebruik van een specifiek type inlogmiddel of tot het beschikbaar stellen van een zakelijke telefoon door de zorg- of jeugdhulpaanbieder.

Met artikel 15 en artikel 7.2.8 van het wetsvoorstel wordt een verplichting voor de zorg- of jeugdhulpaanbieder gecreëerd om alle goedgekeurde inlogmiddelen te accepteren. Dit brengt een keuzevrijheid voor de verschillende inlogmiddelen met zich mee. Het ter beschikking stellen van een zakelijke telefoon is dus niet noodzakelijk voor de genoemde 1,5 miljoen medewerkers.

De eerste ervaringen met Dezi laten zien dat voor bepaalde gebruikersgroepen een fysieke smartcard (vergelijkbaar met de UZI-pas) praktisch blijft, terwijl anderen, bijvoorbeeld in de ambulante omgeving, een voorkeur hebben voor bijvoorbeeld (draadloos uit te lezen) NFC Fido2 passen, de DigiD-app of een wallet op een telefoon of tablet.[18]

28

*De leden van de **GroenLinks-PvdA-fractie** zijn benieuwd of kan worden ingeschat of berekend welk aandeel van deze medewerkers momenteel niet over een zakelijke telefoon beschikt.*

[17] Kamerstukken II 2024-2025, 36 702, nr. 3, blz. 6.

[18] NFC FIDO2 is een technologie waarmee je via een NFC-beveiligingssleutel veilig en zonder wachtwoord kunt inloggen volgens de FIDO2-standaard.

Er kan niet worden ingeschat of berekend welk aandeel van de zorg- en jeugdhulpmedewerkers niet beschikt over een zakelijke telefoon. Deze gegevens worden niet centraal geregistreerd en vallen onder de verantwoordelijkheid van zorg- en jeugdhulpaanbieders. Ik beschik daarom niet over inzicht in deze interne bedrijfsgegevens en acht het ook niet noodzakelijk deze centraal te verzamelen, aangezien het wetsvoorstel niet uitgaat van of stuurt op het gebruik van zakelijke telefoons als voorwaarde voor veilige identificatie en authenticatie. Door het accepteren van meerdere typen inlogmiddelen blijft het stelsel toegankelijk voor zorg- en jeugdhulpmedewerkers, ongeacht de beschikbaarheid van een zakelijke telefoon.

29

*Genoemde leden van de **GroenLinks-PvdA-fractie** 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.*

Het wetsvoorstel biedt ruimte voor het gebruik van verschillende soorten inlogmiddelen, variërend van fysieke passen tot digitale oplossingen, waaronder het gebruik van een smartphone. Er is geen verplichting om een smartphone te gebruiken als inlogmiddel. Het al dan niet beschikbaar stellen van zakelijke telefoons is een keuze van de zorg- en jeugdhulpaanbieder op basis van diens werkproces en staat los van het Dezi-stelsel. De regering ziet dus geen risico bij het niet beschikbaar stellen van een zakelijke telefoon.

Tegelijkertijd ben ik in gesprek met zorg- en koepelorganisaties over het Dezi-stelsel. In deze gesprekken wordt ook aandacht besteed aan praktijkvragen.

Gelet hierop acht ik het niet passend om landelijke richtlijnen op te stellen over het gebruik of het beschikbaar stellen van zakelijke telefoons. Zorg- en jeugdhulpaanbieders verschillen in omvang, organisatievorm en werkwijze, waardoor zij het best in staat zijn om, binnen de wettelijke kaders, zelf afwegingen te maken die aansluiten bij hun specifieke situatie.

30

*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 volgens deze leden ook duidelijk worden hoe werkgevers verwacht worden te voldoen aan de verwachting dat zij alle relevante medewerkers zullen voorzien van een zakelijke telefoon.*

Het wetsvoorstel biedt ruimte voor het gebruik van verschillende soorten inlogmiddelen, variërend van fysieke passen tot digitale oplossingen, waaronder het gebruik van een smartphone. Er is geen verplichting om een smartphone te gebruiken als inlogmiddel. Het al dan niet beschikbaar stellen van zakelijke telefoons is een beleidskeuze van de zorg- en jeugdhulpaanbieder zelf en staat los van het Dezi-stelsel.

Gelet hierop acht ik het niet passend om landelijke richtlijnen op te stellen over het gebruik of het beschikbaar stellen van zakelijke telefoons. Zorg- en jeugdhulpaanbieders verschillen in omvang, organisatievorm en werkwijze, waardoor zij het best in staat zijn om, binnen de wettelijke kaders, zelf afwegingen te maken die aansluiten bij hun specifieke situatie.

31

*De leden van de **GroenLinks-PvdA-fractie** zijn benieuwd of, en zo ja hoe, de verwachting dat zorgaanbieders zakelijke telefoons ter beschikking stellen zijn meegerekend in de verwachte uitvoeringskosten van dit wetsvoorstel. De leden vragen of hiervoor een impactanalyse is opgesteld. Mocht dit niet het geval zijn, dan vragen deze leden of de regering bereid is om alsnog een impactanalyse uit te voeren in samenwerking met de zorgaanbieders. Hierbij vragen deze leden tevens om expliciet stil te staan bij het gebruiken van een zakelijke telefoon door zzp'ers in de zorg.*

Bij de raming van de uitvoeringskosten van dit wetsvoorstel is geen verplichting opgenomen voor zorg- en jeugdhulpaanbieders om zakelijke telefoons aan te schaffen of beschikbaar te stellen aan medewerkers. De zorg- en jeugdhulpmedewerker heeft de keuze tussen verschillende inlogmiddelen en is dus niet gebonden aan een inlogmiddel dat is gekoppeld aan een telefoon. Hierdoor is het beschikbaar stellen van zakelijke telefoons geen noodzakelijke voorwaarde voor de naleving van het wetsvoorstel en zijn eventuele kosten die daarmee samenhangen geen direct gevolg van dit wetsvoorstel.

Voor de implementatie van het Dezi-stelsel is in opdracht van het ministerie van VWS in 2024 door KPMG een onderzoek uitgevoerd naar de verwachte kosten.[19]

Er is geen afzonderlijke impactanalyse opgesteld die specifiek ziet op het gebruik of de aanschaf van zakelijke telefoons. Daarvoor bestaat ook geen aanleiding, aangezien het wetsvoorstel niet verplicht tot het gebruik van een telefoon. Eventuele kosten die samenhangen met het gebruik van telefoon vloeien voort uit keuzes van individuele zorg- en jeugdhulpaanbieders. Het rapport concludeert daarom dat de aanschaf van zakelijke telefoon niet volledig toe te rekenen is aan het Dezi-stelsel.

De regering ziet geen noodzaak om aanvullend een aparte impactanalyse uit te voeren die specifiek is gericht op het gebruik van zakelijke telefoons.
32

[19] KPMG, *Kostenanalyse implementatie generieke functie Identificatie & Authenticatie*, november 2024, link: eindrapport-kostenanalyse-i-a.pdf.

*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. Deze leden vragen als deze telefoon in beheer is van de werkgever, of er dan geen privacyrisico's optreden. Ze vragen daarnaast 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.*

Ik voorzie geen privacy-risico's voor wat betreft het gebruik van een EUDI-wallet op een telefoon die in beheer is van de werkgever.

Beheer houdt in dat bepaalde instellingen kunnen worden voorgeschreven, apps kunnen worden geïnstalleerd of verwijderd, updates kunnen worden uitgevoerd en een toestel op afstand kan worden gewist. Ook kan in bepaalde gevallen worden gezien dát een app is geïnstalleerd. Bij mobile device management wordt de inhoud van de geïnstalleerde apps in beginsel niet uitgelezen. Besturingssystemen van telefoons zijn namelijk zo ingericht dat elke app in een afgesloten omgeving draait, waardoor apps (waaronder mobile device management-software) in beginsel niet onderling toegang tot interne data hebben, tenzij de gebruiker hier expliciet toestemming voor heeft gegeven. Bovendien zij hierbij benadrukt dat de werkgever die een telefoon onder beheer stelt op basis van de AVG verplicht is de betrokkene te informeren over de informatie die daarbij kan worden verwerkt.[20]

Bovendien gelden strenge beveiligingseisen voor de EUDI-wallet. Deze moet namelijk voldoen aan vastgestelde eisen, die transparant gebruik mogelijk maken en waarbij de gebruiker veilige en volledige controle behoudt.[21] Ook moet de wallet op grond van de eIDAS-verordening voldoen aan betrouwbaarheidsniveau hoog, met name wat betreft het bewijzen en het verifiëren van de identiteit en het beheer en de authenticatie van elektronische identificatiemiddelen.

Dit alles is verder uitgewerkt in de Architecture and Reference Framework.[22] Hierin is bepaald dat voor de toegang tot de wallet minimaal twee factorauthenticatie (2FA) vereist.

Dit alles betekent dat de toegang tot de inhoud van de EUDI-wallet niet mogelijk is via de mobile device management zonder dat de zorgmedewerker hierbij betrokken wordt. Bovendien kan een werkgever, die de telefoon in bezit krijgt, zonder de benodigde 2FA-informatie geen toegang krijgen tot de informatie in de wallet.

[20] Artikel 13 van de Algemene verordening gegevensbescherming.

[21] Artikel 5 bis, vierde lid, sub a, van de Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit.

[22] eIDAS Expert Group, *Architecture and reference framework*, November 2023. De ARF beschrijft de gemeenschappelijke normen, richtsnoeren, technische specificaties en best practises die de lidstaten samen ontwikkelen en die gebruikt worden voor informatie-uitwisseling tussen wallets, uitgevers en dienstverleners in de Europese Unie.

33

*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.*

De vaste kosten voor het in stand houden van een gecertificeerde QTSP-dienst zijn over het algemeen vergelijkbaar met de huidige UZI-pas. De kosten voor een middel hangen samen met: het type drager (zoals smartcard, USB-token of mobiel certificaat), de wijze van identiteitsvaststelling van de houder, de wijze van verstrekking, en het volume en aantal diensten waarover de QTSP de vaste kosten kan spreiden. Afhankelijk van deze factoren kunnen de kosten zowel lager als hoger uitvallen dan de huidige UZI-pas. Vanwege lopende technische ontwikkelingen en de verwachting dat er meerdere aanbieders op de markt zullen komen, worden de kosten voor een middel op het hoogste betrouwbaarheidsniveau ingeschat tussen de 20 en 70 euro per jaar. Deze kosten zijn dus niet geheel nieuw. In de huidige situatie maken zorg- en jeugdhulpaanbieders ook kosten voor de aanschaf van inlogmiddelen. Daarnaast wordt benadrukt dat een stijging van beveiligingskosten, zoals voor inlogmiddelen op het hoogste betrouwbaarheidsniveau, onvermijdelijk is gezien het toenemend aantal cyberaanvallen in de zorg. Passende bescherming tegen deze vorm van cybercriminaliteit vereist steeds geavanceerdere beveiligingsmaatregelen, die de nodige kosten met zich meebrengen.

Om zorgorganisaties tegemoet te komen in de aanschaf van nieuwe inlogmiddelen, wordt voor de duur van twee jaar een stimuleringsregeling voorzien.

34

*De leden van de **GroenLinks-PvdA-fractie** lezen in de beantwoording op hun vragen in de nota naar aanleiding van het verslag dat er een stimuleringsregeling van twee jaar wordt voorzien door de overheid om aanschafkosten van nieuwe inlogmiddelen te verlichten. Deze leden vragen ten eerste om hoe veel geld dit gaat, gezien de veel grotere scope dan het gebruik van UZI-passen. De leden van de vragen ten tweede of er na die periode van twee jaar structurele compensatie wordt verzorgd. De leden vragen ten derde 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.*

De regering heeft in totaal 25 miljoen euro beschikbaar gesteld voor een tijdelijke stimuleringsregeling ter ondersteuning van de aanschaf van nieuwe inlogmiddelen. Dit budget is verdeeld over de jaren 2026, 2027 en 2028. De stimuleringsregeling richt zich op het verlagen van de initiële aanschafkosten en is daarmee niet bedoeld om alle kosten volledig te dekken.

Er is niet voorzien in een structurele compensatie voor de periode na afloop van de stimuleringsregeling. De kosten voor het gebruik en beheer van inlogmiddelen worden beschouwd als reguliere bedrijfskosten van zorg- en jeugdhulpaanbieders. De stimuleringsmiddelen hebben als doel om de drempel voor aansluiting op het Dezi-stelsel te verlagen.

De eisen voor het betrouwbaarheidsniveau hoog zijn strikt en voor alle leveranciers gelijk. Het borgen van deze kwaliteit is een randvoorwaarde voor toelating tot het Dezi-stelsel. Omdat deze eisen uniform gelden, ontstaat er een *level playing field*: leveranciers beconcurreren elkaar niet op de veiligheidsnormen, maar op de efficiëntie van hun bedrijfsvoering, gebruiksgemak van het middel, innovatie en dienstverlening.

Daarbij wordt de rol van marktwerking versterkt door de aansluiting bij de status van QTSP zoals volgt uit de eIDAS-verordening. Een QTSP voldoet al grotendeels aan de eisen van de NEN 7518.[23] Grotendeels, omdat de NEN 7518 in aanvulling op de eisen voor de betrouwbaarheid uit de Uitvoeringsverordening (EU)2015/1502, extra eisen stelt voor de interactie met het Dezi-stelsel,
bijvoorbeeld over de wijze waarop de zorgidentiteit wordt verkregen van het CIBG uit het Dezi-register. Doordat de leverancier van het (technische) middel al gecertificeerd is als QTSP, kan de informatie van die certificering worden hergebruikt en daarmee de certificering als zorgspecifiek middel op basis van de NEN 7518 sneller doorlopen worden. Hierdoor kunnen QTSP's hun bestaande infrastructuur benutten, wat schaalvoordelen oplevert en de drempel voor markttoetreding verlaagt.

Kortom: de regering borgt de kwaliteit via strikte eisen, terwijl de marktwerking binnen deze kaders zorgt voor kostenefficiëntie door concurrentie op prijs en procesoptimalisatie.

Sinds oktober 2025, heeft de NEN op verzoek van het veld een aanvulling voorbereid op de (concept-) norm NEN 7518. Deze aanpassing maakt het mogelijk om ook een zorgspecifiek middel uit te geven met behulp van de leverancier van het middel die géén QTSP-status heeft. Voorwaarde hierbij is dat het inlogmiddel aantoonbaar voldoet aan dezelfde eisen voor betrouwbaarheidsniveau hoog, zoals vastgelegd in de Uitvoeringsverordening (EU) 2015/1502. Hiermee is beoogd eventuele onvoorziene negatieve effecten als gevolg van kosten voor compliance van QTSP's uit te sluiten.

Hiermee wordt tegemoetgekomen aan de wens uit de zorgsector om flexibiliteit in het aanbod van middelen te behouden, mits de veiligheid gewaarborgd blijft. Het toetsen of een middel aan de Uitvoeringsverordening (EU)2015/1502 eisen voor betrouwbaarheidsniveau hoog voldoet, vereist een onafhankelijke audit. Hoewel dit proces inhoudelijk lijkt op QTSP-certificering, is het beperkter en biedt het een alternatieve route voor partijen die wel een middel willen inzetten dat aan de eisen voor betrouwbaarheidsniveau voldoet, maar als organisatie niet de formele Europese status van QTSP willen.

Overheid

35

*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. Deze leden vragen daarom aan de regering hoe voorkomen gaat worden dat de nieuwe zorgspecifieke inlogmiddelen niet dezelfde gebruiksproblemen krijgen als de UZI-pas.*

Het wetsvoorstel bevat bewust geen bepalingen over op de verschijningsvorm (zoals een pas) van de te ontwikkelen inlogmiddelen. Op die manier wordt niet alleen innovatie mogelijk gemaakt, er wordt bovendien tegemoetgekomen aan het feit dat de eisen aan middelen vanuit de zorg niet uniform zijn.

De aanleiding voor leveranciers om een middel in de vorm van een 'insteekpas' te ontwikkelen, zoals bij de introductie van deze vraag wordt opgemerkt, ligt vermoedelijk in het feit dat zorgspecifieke middelen in de NEN 7518 ook bruikbaar moeten zijn voor het zetten van een gekwalificeerde elektronische handtekening. Traditioneel wordt hierbij een smartcard als technische oplossing toegepast. Dat hoeft echter niet omdat het technisch ook mogelijk is gekwalificeerde elektronische handtekeningen te zetten zonder gebruik van een smartcard. Het aandachtspunt is in de NEN-werkgroep besproken. Op verzoek van de werkgroep heeft de NEN een aanvulling voorbereid op de (concept)norm NEN 7518. Hierin wordt verduidelijkt dat het elektronisch

[23] 'grotendeels' omdat de NEN 7518 in aanvulling op de eisen voor de betrouwbaarheid uit (EU)2015/1502, extra eisen stelt voor de interactie met het Dezi-stelsel bijvoorbeeld over de wijze waarop de zorgidentiteit wordt verkregen van het CIBG uit het Dezi-register.

ondertekenen ook zo kan worden ingericht dat het tekenen 'buiten het middel' wordt uitgevoerd, dus met een *remote Qualified Electronic Signature Creation Device*.[24] Deze uitleg maakt duidelijk dat er geen noodzaak is voor een smartcard.

Hierbij wordt opgemerkt dat bekend is dat een leverancier van een traditioneel smartcard-middel beoogt een zorgspecifiek middel te ontwikkelen en te certificeren via de NEN 7518. Ook is duidelijk geworden dat twee QTSP's een 'wallet'-oplossing willen aanbieden en een andere leverancier een combinatie van een 'wallet en smartcard' wil gaan aanbieden voor de processen en werkomstandigheden waar de insteekpas-vorm juist zeer gewaardeerd wordt. Met deze oplossingen zullen goede alternatieven worden geboden die de gebruiksproblemen van de UZI-pas kunnen ondervangen.

36

*De leden van de **GroenLinks-PvdA-fractie** vragen welke problemen de regering ziet met de gebruiksvriendelijkheid van de UZI-pas en hoe de regering deze problemen specifiek wegneemt.*

Een van de problemen met de UZI-pas is dat het niet gebruiksvriendelijk is en niet past binnen elk werkproces. De UZI-pas (met bijbehorende kaartlezer) werkt namelijk niet op mobiele apparaten zoals een smartphone of tablet en is daarmee niet voor ieder werkproces geschikt. Te denken valt aan zorgprocessen in de ambulancezorg en de ambulante zorg (thuiszorg) waar met mobiele apparaten gewerkt wordt.

Daarnaast is de huidige UZI-pas niet flexibel doordat de zorgidentiteit van de professional in het UZI-register, bestaande uit een uniek nummer, de werkgever-werknemer relatie en de rolcode op basis van het beroep dat een professional uitoefent, fysiek op de chip van de UZI-pas is geprint. Als er een wijziging plaatsvindt in werkgever-werknemer relatie of beroep, is er daarom een nieuw middel nodig. Dat brengt naast administratieve lasten ook de nodige kosten met zich mee.

Door te bepalen dat middelen aan betrouwbaarheidsniveau hoog moeten voldoen, ontstaan mogelijkheden voor verschillende soorten veilige inlogmiddelen en kan innovatie van de markt worden gebruikt om inlogmiddelen verder te verbeteren. Hierdoor kan betere aansluiting worden gevonden voor middelen op werkprocessen die bijvoorbeeld in een administratieve omgeving anders kunnen zijn dan in een ambulante setting of voor het werken in een hygiënische ruimte. Door het mogelijk te maken om de zorgidentiteit op te halen op het moment van inlog, in plaats van deze hard op/in het middel te plaatsen, zijn wijzigingen in het register (zoals een wijziging in werkgever-werknemer relatie of beroep) direct beschikbaar en hoeven geen nieuwe middelen (fysiek) te worden uitgereikt en kunnen zorg- en jeugdhulpmedewerkers sneller aan de slag.

[24] Zie ook artikel 3, onderdeel 23, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU2014,* L257/73). Dit is een inlogmiddel voor het aanmaken van een elektronisch handtekeningen.

Burgers

37

*De leden van de **GroenLinks-PvdA-fractie** geven aan grote waarde te hechten aan het inzagerecht van patiënten in hun gegevens. Deze leden geven aan dat in de beantwoording bij de nota naar aanleiding van het verslag 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.*
De scope en het doel van het onderzoek is om te bezien of de burgerrechten, waaronder het inzagerecht kan worden vormgegeven en gefaciliteerd via een Dienst voor Toegang. Hierbij wordt onder ander gekeken naar de technische haalbaarheid en praktische uitvoerbaarheid. In de Kamerbrief EHDS van januari 2026 is toegezegd dat de Kamer na de zomer geïnformeerd wordt over het gehele stelsel aan burgerrechten.[25]

Hierbij zij opgemerkt dat dit onderdeel niet valt onder de scope van het wetsvoorstel. Het wetsvoorstel ziet namelijk niet op het inzagerecht van burgers, maar op de identificatie en authenticatie van met name zorg- en jeugdhulpaanbieders en hun medewerkers.

Werkbare invoering in de praktijk

38

*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 van de nota naar aanleiding van het verslag. Genoemde leden vragen de regering te bevestigen dat zorgmedewerkers zich inderdaad slechts één keer per dag 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.*

Het aantal keer dat moet worden ingelogd is afhankelijk van het beleid van de individuele zorg- of jeugdhulpaanbieder, dat beleid moet voldoen aan de NEN 7510 en de eIDAS-verordening.

Het inloggen in applicaties kent twee stappen. Na de authenticatie wordt eerst een authenticatieverklaring afgegeven door het Dezi-register. Dit bewijs wordt aan de (applicatie van de) zorg- of jeugdhulpaanbieder aangeboden die vervolgens een ‘sessie’ start en op grond van rechten toegang verleent aan de zorg- of jeugdhulpmedewerker. Het is daarbij aan de zorg- of jeugdhulpaanbieder om vast te stellen wat de maximale duur wordt van een sessie en van inactiviteit. Deze termijnen worden bepaald op basis van een risicoanalyse die de zorg- of jeugdhulpaanbieder zelf (verplicht) moet uitvoeren om te voldoen aan de NEN 7510. Hierbij spelen ook de eisen uit de eIDAS-verordening een rol. Hierin is namelijk bepaald dat voor middelen op betrouwbaarheidsniveau hoog dynamische authenticatie is vereist.[26] Dit betekent dat voor toegang tot diensten/gegevens authenticatiebewijzen niet hergebruikt mogen worden. Wanneer een zorg- of een jeugdhulpmedewerker voor de behandeling toegang zoekt tot verschillende diensten of bronnen,

[25] Kamerstukken 2025-2026, 27529, nr. 356.

[26] Artikel 1, onderdeel 3 & paragraaf 2.3.1 van het Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (*PbEU* 2015, L 235/7).

bijvoorbeeld ook bij bronnen buiten de eigen organisatie, dan kan daarom een herauthenticatie gevraagd worden. De wijze waarop de gegevensuitwisseling is ingericht, is hierin bepalend en kan voorkomen dat de medewerker hernieuwd moet authentiseren, maar sluit dat niet uit.

Dit alles betekent dat het aan de zorg- of jeugdhulpaanbieder is of en wanneer herauthenticatie moet plaatsvinden, bijvoorbeeld na twee of vier uur, of na het wisselen tussen dossiers. Het Dezi-stelsel is hier in de basis niet limiterend in.

De genoemde structurele administratieve lastenverlichting ziet toe op de standaardisatie en centralisatie van het beheer van inlogmiddelen. Waar zorg- en jeugdhulpaanbieders momenteel vaak nog kampen met bewerkelijk lokaal uitgiftebeheer en dubbele registraties, zorgt een persoonsgebonden inlogmiddel voor een efficiënter proces. Zo kunnen publieke inlogmiddelen onder de Wdo en eIDAS-verordening worden gebruikt. Dit voorkomt dat instellingen zelf nieuwe middelen moeten aanschaffen en uitrollen, terwijl zorg- en jeugdhulpprofessionals niet langer verschillende inlogmiddelen (zoals pasjes) voor verschillende werkgevers hoeven te beheren.

Hoewel de overstap naar het Dezi-stelsel op de korte termijn een incidentele investering vraagt voor de technische aansluiting, wijst het in opdracht van mijn ministerie uitgevoerde onderzoek van KPMG uit dat de kosten per gebruiker dalen door dit vereenvoudigde beheer.[27]

39

*De leden van de **GroenLinks-PvdA-fractie** hebben dezelfde vraag over het zetten van een digitale handtekening, bijvoorbeeld voor recepten en consulten. De leden geven aan dat dit handelingen zijn 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 noodzaak tot het zetten van een digitale handtekening, bijvoorbeeld voor recepten en consulten, en de vereisten die daarvoor gelden, volgen uit de norm NEN 7510, de Geneesmiddelenwet en de AVG. Het wetsvoorstel brengt hier geen verandering in.

De NEN 7510 vereist dat de zorg- en jeugdhulpaanbieder borgt dat documenten en gegevens in applicaties zodanig zijn beveiligd, dat kan worden aangetoond dat deze niet nadien zijn aangepast. Eén van de technische beheersmaatregelen om deze onweerlegbaarheid te borgen is het toepassen van cryptografie via digitale ondertekening. Uit artikel 1 lid 1 sub pp van de Geneesmiddelenwet volgt dat een recept voor bepaalde categorieën geneesmiddelen moet zijn ondertekend door de desbetreffende beroepsbeoefenaar, of met een zodanige code moet zijn beveiligd zodat een daartoe bevoegde persoon of instantie de authenticiteit ervan kan vaststellen. Tot slot zijn zorg- en jeugdhulpaanbieders op grond van artikel 32 AVG verplicht passende organisatorisch en technische maatregelen te treffen. Nu het hierbij gaat om medische gegevens, die vallen onder het medisch beroepsgeheim, wordt betrouwbaarheidsniveau hoog passend geacht.[28]

Het voorgaande leidt ertoe dat de zorg- en jeugdhulpaanbieder ook nu al, gehouden is om gebruik te maken van de gekwalificeerde elektronisch handtekening, omdat anders niet wordt voldaan aan de NEN 7510, de Geneesmiddelenwet en de AVG. Dit type handtekening voldoet immers aan het hoogste betrouwbaarheidsniveau en wordt gelijkgesteld aan de “natte handtekening” in de zin artikel 3:15a van het Burgerlijk Wetboek.

---

[27] KPMG, *Kostenanalyse implementatie generieke functie Identificatie & Authenticatie*, november 2024, link: eindrapport-kostenanalyse-i-a.pdf.

[28] Brief Autoriteit Persoonsgegevens d.d. 4 oktober 2018 met kenmerk z2018-17577 en Kamerstukken II 2016-2017, 27 529, nr. 143, blz. 1.

Voor het zetten van een gekwalificeerde elektronische handtekening is vereist dat elke afzonderlijke keer wordt aangetoond dat dit gebeurt onder exclusieve controle van de ondertekenaar. Onder het huidige regime van de UZI-pas gebeurt dit bijvoorbeeld door de pincode te vragen die hoort bij de pas waarop het certificaat staat waarmee wordt getekend.
Met het wetsvoorstel worden geen veranderingen aangebracht ten aanzien van de eIDAS-vereisten aan gekwalificeerde handtekeningen. Ook de NEN 7510, de AVG en de Geneesmiddelenwet blijven ongewijzigd. Het wetsvoorstel brengt daarom op dit punt geen forse toename aan administratieve lasten met zich mee.

40

*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 de leden om nader toe te lichten welke verkenning voor de implementatie op de BES-eilanden er nu plaatsvindt. De leden vragen daarnaast op welke termijn deze verkenning is afgerond.*

Met de leden van de fractie van GroenLinks-PvdA deel ik het uitgangspunt van een gelijkwaardige bescherming van persoons- en patiëntgegevens in heel het Koninkrijk. De digitale infrastructuur in Caribisch Nederland is nog aan het ontwikkelen en in technische zin nog niet vergelijkbaar met de digitale infrastructuur in Europees Nederland. Wel zijn er meerdere digitaliseringstrajecten in de zorgsector gestart. Voor implementatie van voorliggend wetsvoorstel is het echter nog te vroeg. Ik blijf in gesprek met de bestuurders van de BES-eilanden om te bezien of, hoe en wanneer aansluiting mogelijk en wenselijk is. Een termijn kan ik echter nu nog niet geven.

41

*De leden van de **GroenLinks-PvdA-fractie** vragen wat gaat de regering gaat doen als blijkt dat er aanvullende maatregelen nodig zijn om het Dezi-stelsel op de BES-eilanden in te voeren? Zij zijn benieuwd of dit om mogelijk aanpassingen van dit wetsvoorstel vraagt.*

Als aansluiting bij het DEZI-stelsel op de BES-eilanden mogelijk is, zal op dat moment worden onderzocht wat hiervoor in organisatorische, technische en juridische zin nodig is. De noodzaak van aanpassing van de wet- en regelgeving zal van dit onderzoek deel uitmaken. Het is echter nog te vroeg om hier in voorliggend wetsvoorstel op vooruit te lopen.

Vragen en opmerkingen van de leden van de CDA-fractie

Nota naar aanleiding van het verslag

42

*De leden van de **CDA-fractie** 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. De leden van de CDA-fractie begrijpen dat dit waarborgen biedt, maar vragen of dit voldoende is, zeker gezien de actuele (geopolitieke) ontwikkelingen. Deze leden vragen daarnaast 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.*

Het kabinet heeft uiteraard oog voor de actuele (geopolitieke) ontwikkelingen en de vraag of er meer nodig is om de cyber security op een voldoende niveau te handhaven voor de zorgsector. De plannen die ik daarvoor heb zijn in december 2025 uiteengezet in de brief over Informatie- en Communicatietechnologie in de Zorg.[29]
Bestaande Europese en nationale kaders bieden handvatten voor strategische autonomie en nationale veiligheid. Europese inlogmiddelen die binnen het toepassingsgebied van dit wetsvoorstel worden gebruikt, moeten voldoen aan de eisen uit de eIDAS-verordening en de daarop gebaseerde toezicht- en certificeringskaders.

Het kabinet onderschrijft dat het van belang is dat Nederland controle houdt over vitale digitale infrastructuur, zeker in sectoren zoals de zorg. Daarom zijn er contractueel afspraken gemaakt tussen het CIBG en private partijen over de locatie van de data en de bescherming ervan. Via een preferente aandelenconstructie is de leverancier beschermd tegen vijandige overnames, wat moet voorkomen dat de gegevens alsnog buiten de EU bewaard, ingezien of gebruikt kunnen worden. Ook zijn er aanvullende afspraken gemaakt over hoe er gehandeld dient te worden wanneer een niet-Nederlandse overheidsdienst om gegevens verzoekt. Tot slot bevat de ARBIT-2018 de mogelijkheid tot ontbinding indien er sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van de leverancier. Bij een ontbinding kan verzocht worden om retournering van de data.

Het kabinet werkt met een risico-gerichte aanpak aan onze strategische autonomie, op nationaal en Europees niveau. In het kader van digitale soevereiniteit is in december 2025 de Visie Digitale autonomie van de overheid vastgesteld.[30] Hierin staat de strategische richting waarmee de Nederlandse overheid haar digitale autonomie en haar digitale soevereiniteit kan versterken, onder andere door het beperken van de afhankelijkheden van niet Europese digitale aanbieders. Binnen de Nederlandse Digitaliseringsstrategie (NDS) is digitale weerbaarheid en autonomie één de prioriteiten waarop wordt ingezet.[31]

Zorg- en jeugdhulpaanbieders zijn zelf verantwoordelijk voor hun IT-infrastructuur. Het CIBG levert wel diensten namens mijn ministerie. Als stelselverantwoordelijke onderneem ik ook stappen om de veiligheid van deze IT-infrastructuur verder te verstevigen. Zoals aangegeven in de brief over Informatie- en Communicatietechnologie in de Zorg[32] doe ik dit onder meer door het bevorderen van bewustzijn, het bieden van passende ondersteuning, het verschepen van toezicht en het bieden van begeleiding bij incidenten.[33]

[29] Kamerstukken II 2025-2026, nr. 353.

[30] Visie Digitale autonomie en soevereiniteit van de overheid, 30 juni 2025, link: Visie - Digitale autonomie en soevereiniteit van de overheid.

[31] De Nederlandse Digitaliseringsstrategie, juni 2025, link: De Nederlandse Digitaliseringsstrategie.

[32] Kamerstukken II 2025-2026, nr. 353.

[33] Kamerstukken II 2025-2026, nr. 353.

43

*De leden van de **CDA-fractie** 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.*

Het wetsvoorstel erkent inlogmiddelen op betrouwbaarheidsniveau hoog vanuit de Wdo, eIDAS-verordening, PKI-O en op basis van de NEN 7518. Deze kaders beschrijven allen de eisen waaraan een middel op betrouwbaarheidsniveau hoog moet voldoen. Deze kaders verwijzen naar de eIDAS-verordening en naar Uitvoeringsverordening (EU) 2015/1502 waarin minimale technische specificaties en procedures voor het betrouwbaarheidsniveau voor elektronische identificatiemiddelen zijn vastgelegd.

Bovendien staan de Wdo-middelen en het PKI-O-afsprakenstelsel onder toezicht van het ministerie van BZK en de zorgspecifieke inlogmiddelen onder toezicht van de Inspectie Gezondheidszorg en Jeugd. Daarnaast staan de eisen van naleving van de eIDAS-verordening, waaronder de regels voor de QTSP, onder toezicht van de EU.

Het wetsvoorstel beoogt een open stelsel te zijn waarin keuzevrijheid is van de erkende middelen. De regering is niet voornemens een specifiek middel te stimuleren, dat zou de marktwerking in dit open stelsel niet ten goede komen.

44

*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. De 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.*

Het is belangrijk om te benadrukken dat DigiD een inlogmiddel is, terwijl eHerkenning een stelsel is. DigiD is op dit moment het enige (publieke) inlogmiddel onder de Wdo waarmee burgers online toegang kunnen krijgen tot overheidsdienstverlening. Binnen dit wettelijk kader is op grond van artikel 9 van de Wdo (nog niet inwerking getreden) voorgesorteerd op een stelsel met keuzevrijheid, met daarin een keuzemogelijkheid voor private inlogmiddelen. De Wdo maakt het dus mogelijk dat er in de toekomst ook meerdere inlogmiddelen in het burgerdomein kunnen worden toegelaten. Het is dus niet correct dat voor de Wdo ‘gekozen is voor één middel’. Deze beoogde erkenning van verschillende private identificatiemiddelen vertoont hiermee sterke gelijkenissen met de uitgangspunten van het voorliggende wetsvoorstel waarbij publieke en erkende private middelen kunnen worden gebruikt voor de zorg.

Het stelsel van eHerkenning is een privaat-publiek stelsel binnen het bedrijvendomein waarbij verschillende inlogmiddelen beschikbaar zijn. De leverancier van een inlogmiddel kan niet zomaar toetreden, maar moet voldoen aan eisen om een erkende leverancier te worden. De overheid is eigenaar van het stelsel en de leveranciers van de inlogmiddelen zijn privaat. Binnen dit stelsel zijn er marktpartijen uit zowel Europese alsook niet-Europese landen die inlogmiddelen aanbieden. Wel zijn alle aanbieders in Nederland gevestigd. Bedrijven die een eHerkenningsmiddel kopen, kunnen daarbij gemakkelijk overstappen. Afhankelijkheid van niet-Europese marktpartijen is dan ook gering. Het is dus niet correct dat voor de eHerkenning is gekozen ‘voor een aantal erkende leveranciers’. De opzet van eHerkenning als een open stelsel met erkenning van verschillende identificatiemiddelen op basis van een normenkader (‘Afsprakenstelsel eHerkenning’) waardoor er een ‘multi-middelen’-oplossing bestaat, vertoont hiermee

sterke gelijkenissen met de uitgangspunten van het voorliggende wetsvoorstel waarbij publieke en erkende private middelen kunnen worden gebruikt.

Het is juist dat in het wetvoorstel niet is gekozen voor één inlogmiddel. Welk inlogmiddel het meest geschikt is, hangt onder andere af van de bedrijfsvoering van een zorg- of jeugdhulpaanbieder en de bij deze organisatie bestaande digitale infrastructuur.

45

*De leden van de **CDA-fractie** 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.*
Er is niet voor gekozen om een aantal erkende leveranciers aan te wijzen. De veiligheid en betrouwbaarheid van de inlogmiddelen wordt gebaseerd op de toelatingen in de kaders van de Wdo, de eIDAS-verordening, PKI-O afsprakenstelsel en de NEN 7518. Deze kaders stellen direct of indirect de eisen zoals gesteld in de Uitvoeringsverordening (EU) 2015/1502 en verlangen dat aantoonbaar hieraan is voldaan.

Er wordt niet verwacht dat er een wildgroei aan inlogmiddelen zal ontstaan gezien de strikte eisen aan middelen. Bovendien wordt met het wetsvoorstel uitsluitend het zorgspecifieke middel, dat onder de verantwoordelijkheid van de zorg- of jeugdhulpaanbieder wordt ontwikkeld, als nieuw inlogmiddel geïntroduceerd. Alle overige middelen zullen immers worden erkend op basis van een nationaal kader (Wdo en PKI-O-afsprakenstelsel) of een EU-kader (eIDAS-verordening).

Nota van Wijziging: Onderdelen G en H

46

*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.*

De aanpassing door de nota van wijziging, die door u is ontvangen op 7 oktober 2025, betrof slechts een wetstechnische wijziging. Het doel van deze wijziging was om te verduidelijken dat de verplichtstelling bij de inwerkingtreding van het wetsvoorstel nog niet van toepassing is.

De wijzigingsbepaling in het oorspronkelijke wetsvoorstel bevatte namelijk in hetzelfde artikel zowel de mogelijkheid (een *kan-bepaling*), als de verplichting om goedgekeurde inlogmiddelen te gebruiken. Een vrijblijvende mogelijkheid en een verplichting in hetzelfde artikel leidt tot onduidelijkheid. Er is expliciet gemaakt dat er eerst een overgangsperiode van toepassing, waarna per 1 januari 2031 de verplichtstelling van het gebruik van goedgekeurde inlogmiddelen gaat gelden. De nota van wijzing maakt mogelijk dat de verplichtstelling via een koninklijk besluit van toepassing verklaard kan worden. Het streven blijft om de verplichtstelling op 1 januari 2031 in te laten gaan.

47

*De leden van de **CDA-fractie** 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.*

Er is gekozen voor een overgangsperiode tot 1 januari 2031 om zorg- en jeugdhulpaanbieders, leveranciers en andere betrokken partijen voldoende tijd te geven om hun systemen aan te passen en de implementatie van het Dezi-stelsel beheerst te laten plaatsvinden.
Het naar voren halen van de datum brengt het risico met zich mee dat niet alle partijen tijdig kunnen voldoen aan de verplichting, wat de continuïteit van de zorg kan raken. Het vervroegen van de datum is daarom niet wenselijk. Wel wordt ingezet op stimulering van snelle implementatie van het Dezi-stelsel.

Vragen en opmerkingen van de leden van de BBB-fractie

48
*De leden van de **BBB-fractie** vragen in hoeverre de gevolgen voor kleine zorgaanbieders, zoals zelfstandige praktijken, wijkzorgteams en kleinschalige jeugdhulpaanbieders, realistisch zijn ingeschat.*

Bij de voorbereiding van dit wetsvoorstel is bij zorgkoepels actief de toekomstvisie op de identificatie en authenticatie van de zorg- en jeugdhulpverlener opgehaald. Dit heeft geleid tot inzicht in belemmeringen en behoeftes aan een toekomstige oplossing die tijdens de uitwerking via Dezi worden vormgegeven.

De inhoud van het wetsvoorstel is bij de voorbereiding ook voorgelegd aan de klankbordgroepen van Dezi. In deze klankbordgroep hebben vertegenwoordigers van de verschillende zorgaanbieders deelgenomen.

Om de gevolgen voor zorg- en jeugdhulpaanbieders in te schatten, is bij de voorbereiding van het wetsvoorstel gekeken naar de volle breedte van het veld. Daarbij is niet uitsluitend naar omvang van organisaties gekeken, maar vooral naar type processen, gegevensuitwisseling en bestaande ICT-inrichting. Ook de kleine zorgaanbieders waren derhalve onderdeel van deze verkenning.
Uit het onderzoek bleek dat niet alleen grote, maar ook veel kleine zorgaanbieders nu al gebruikmaken van inlogmiddelen en toegangsvoorzieningen. In veel gevallen zal het wetsvoorstel daarom niet leiden tot het volledig nieuw invoeren van middelen of processen, maar eerder tot een aanpassing of de vervanging van bestaande middelen en processen. De tijdelijke stimuleringsregeling voor de aanschaf van nieuwe inlogmiddelen van in totaal 25 miljoen euro gaat hierbij ondersteuning bieden.

Verder is er een centrale test- en pilotomgeving om ketenproeven te doen met zorginstellingen, middelenleveranciers en softwareleveranciers. Hiermee worden potentiële implementatiebelemmeringen qua proces, techniek en beheer vóór brede uitrol ondervangen, zodat de implementatielast verder daalt.

Tot slot geldt dat de invoering gefaseerd wordt voorbereid. Ten eerste het tijdig beschikbaar komen van heldere implementatieproducten, zoals: standaarden, aansluitprofielen, testmogelijkheden, handreikingen en support. Ten tweede door het oplossen van eventuele onbedoelde knelpunten voor kleine zorgaanbieders die via pilots belicht worden voordat bredere verplichtingen ingaan.

49

*De leden van de **BBB-fractie** vragen welke uitvoeringsproblemen de regering specifiek verwacht bij kleinere zorgaanbieders, en welke ondersteuning komt beschikbaar om deze verplichtingen haalbaar te maken.*

Bij kleinere zorgaanbieders kunnen zich specifieke uitvoeringsuitdagingen voordoen. Zo is er vaak sprake van beperkte ICT-capaciteit en veranderkracht. Zij hebben namelijk vaak geen eigen ICT-team en hebben

hierdoor minder ruimte om projecten te plannen, testen en uit te rollen. De kleine zorg- en jeugdhulpaanbieders worden hierin ondersteund door leveranciers van de elektronische patiëntendossiers, huisartseninformatiesystemen, jeugdsystemen en portalen. Zij bieden namelijk standaard-koppelingen en configuratie-opties aan. Hoewel dit enerzijds afhankelijkheid met zich meebrengt, biedt het anderzijds een kostenbesparende oplossing, omdat (duur) maatwerk wordt voorkomen en standaard ondersteuning vanuit de leverancier beschikbaar komt.

Ook de kosten voor de aanschaf van nieuwe inlogmiddelen kunnen relatief zwaarder zijn voor kleinere zorg- en jeugdhulpaanbieders. Om deze lasten te drukken, kan gebruik worden gemaakt van de tijdelijke stimuleringsregeling van 25 miljoen euro. Verder worden concrete implementatieproducten ontwikkeld, zoals handreikingen, minimale beheerprocessen, voorbeeldteksten en werkinstructies, die kleine aanbieders ondersteunen bij de invoering van Dezi.

50

*De leden van de **BBB-fractie** vragen of inzichtelijk gemaakt kan worden welke eenmalige en structurele kosten kleine zorgaanbieders moeten maken om aan dit systeem te voldoen.*

De exacte administratieve lasten en kosten voor identificatie en authenticatie zijn kwantitatief niet te duiden, maar zullen voor een groot deel afhankelijk zijn van het inlogmiddel.

Daarnaast zijn er eenmalige kosten voor het aansluiten van de elektronische- en zorginformatiesystemen op het Dezi-stelsel, zoals voor: het technisch koppelen met het Dezi-authenticatieplatform, het kunnen verwerken van zorgidentiteitsgegevens en het koppelen van de zorgidentiteitsgegevens aan de bestaande medewerkers en autorisaties in de systemen. Naar verwachting worden de zorg- en jeugdhulpaanbieders hierbij ondersteund door de platformleveranciers. Ook het aanschaffen van middelen voor de zorg- en jeugdhulpmedewerkers is een kostencomponent.

Er zijn ook periodieke kosten, opgebouwd uit: administratie lasten om de registraties van werknemer-werkgever in het Dezi-register actueel te houden, kosten voor de registratie van zorg- of jeugdhulpaanbieder en zorg- of jeugdhulpmedewerker in het register, kosten voor het inlogmiddel en beheer- en onderhoudslasten van de platformleverancier voor de aansluiting op het Dezi-stelsel.

Daarbij is wel van belang dat het voorliggend wetsvoorstel niet los staat van de bestaande digitale infrastructuur. Zorg- en jeugdhulpaanbieders maken nu ook al kosten voor hun ICT-systemen, toegangsbeheer en inlogmethoden. In veel gevallen zal sprake zijn van aanpassingen of vervanging van bestaande oplossingen, en niet van volledig nieuwe voorzieningen.

51

*De leden van de **BBB-fractie** vragen hoe de regering voorkomt dat aanbieders afhaken of stoppen omdat deze ICT-verplichtingen voor hen niet uitvoerbaar of betaalbaar zijn.*

Ik verwacht niet dat zorg- en jeugdhulpaanbieders ingevolge het wetsvoorstel stoppen vanwege ICT-verplichtingen. Bij de vormgeving van het wetsvoorstel is rekening gehouden met de uitvoerbaarheid. Daarom is er gekozen voor een overgangs- en implementatieperiode, gefaseerde invoering en aansluiting op bestaande standaarden en erkende middelen.

Daarnaast wordt gewerkt met pilots, waarbij samen met zorg- en jeugdhulpaanbieders en leveranciers wordt beproefd welk inlogmiddel passend is bij de verschillende werkprocessen. De ervaringen uit deze pilots worden gebruikt om de implementatiestrategie waar nodig bij te stellen, knelpunten te signalen en oplossingen te ontwikkelen voor de landelijke opschaling.
Verder stelt de regering tijdelijke stimuleringsmiddelen van in totaal 25 miljoen euro beschikbaar voor het aanschaffen van inlogmiddelen door zorg- en jeugdhulpaanbieders en 8 miljoen euro voor het koppelen van ICT-systemen door ICT-leveranciers. Hiermee zorgt de regering ervoor dat aansluiting op het Dezi-stelsel betaalbaar blijft.
52

*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. De 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?*

De eerste nota van wijziging, aangeboden aan uw Kamer op 7 oktober 2025, wijzigt Artikel I, onder F, en Artikel II, onder B. In deze nota van wijziging is toegelicht dat de datum van 1 januari 2029 is vervroegd naar 1 november 2028. Deze wijziging hangt samen met het verlopen van de stamcertificaten op 1 november 2028.[34] Het CIBG geeft namelijk UZI-middelen uit op basis van deze stamcertificaten. Wanneer de oorspronkelijke datum zou worden aangehouden, dan zou het CIBG twee maanden nieuwe UZI-middelen moeten uitgeven en aanschaffen onder de nieuwe stamcertificaten. Zorgpartijen zouden dan nieuwe UZI-middelen aanschaffen voor de periode van maar twee maanden. Door de einddatum te vervroegen, loopt de duale periode gelijk met het aflopen van de huidige stamcertificaten.

Een ander onderdeel van die nota van wijziging betrof daarnaast een wetstechnische wijziging om te verduidelijken dat de verplichtstelling bij de inwerkingtreding van het wetsvoorstel nog niet van toepassing is.

De wijzigingsbepaling in het oorspronkelijke wetsvoorstel bevatte namelijk in hetzelfde artikel zowel de mogelijkheid (een *kan-bepaling*), als de verplichting om goedgekeurde inlogmiddelen te gebruiken. Een vrijblijvende mogelijkheid en een verplichting in hetzelfde artikel leidt tot onduidelijkheid bij de praktijk. In lijn met het voornemen van dit wetsvoorstel is eerst een overgangsperiode van toepassing, waarna per 1 januari 2031 de verplichtstelling van het gebruik van goedgekeurde inlogmiddelen gaat gelden. De nota van wijzing maakt mogelijk dat de verplichtstelling per koninklijk besluit van toepassing verklaard kan worden.

53

*De leden van de **BBB-fractie** vragen of de regering kan garanderen dat de sector tijdig beschikt over voldoende goedgekeurde inlogmiddelen voordat verplichtingen ingaan.*

Op dit moment is al een publiek middel beschikbaar onder de Wdo. Het is de verwachting dat ook tijdig zorgspecifieke middelen zullen worden aangeboden. Hierover lopen momenteel gesprekken met leveranciers en koepel- en zorgorganisaties.

[34] Een stamcertificaat is het ankerpunt voor vertrouwen in elektronische transacties van en met de overheid bij het vaststellen van identiteit, het afgeven van wilsuitingen en het vertrouwelijk communiceren. Zie ook: Staatscourant 2024, 37801.

Tot slot ontwikkelt het ministerie van BZK momenteel de NL-Wallet. Dit is een digitale wallet onder het EUDI-stelsel. Deze wallet zal op het moment van de verplichtstellingen uit het wetsvoorstel beschikbaar zijn.

54

*De leden van de **BBB-fractie** vragen hoe wordt voorkomen dat zorgaanbieders halverwege moeten overstappen omdat eerdere planning onrealistisch bleek.*

In het wetsvoorstel is, mede na het advies van de Afdeling advisering van de Raad van State, een verplichtstelling per 1 januari 2031 voor het Dezi-stelsel opgenomen. [35] De tijd tussen de inwerkingtreding van het wetsvoorstel en deze verplichtstellingsdatum is de implementatieperiode. Deze periode is bedoeld om zorg- en jeugdhulpaanbieders, leveranciers en ketenpartijen voldoende tijd te geven om de benodigde aanpassingen zorgvuldig en beheerst door te voeren. Hiervoor vindt momenteel al communicatie plaats.

Om te voorkomen dat partijen halverwege moeten overstappen als gevolg van bijgestelde planningen, worden pilots toegepast om de landelijke invoering waar nodig bij te sturen.

55

*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. Deze leden vragen of de regering bereid is een risicoanalyse te delen over het scenario waarin goedgekeurde inlogmiddelen niet tijdig beschikbaar zijn.*

Er is geen risicoanalyse gedaan op het scenario waarin goedgekeurde inlogmiddelen niet tijdig beschikbaar zijn. Op dit moment is namelijk al een publiek middel beschikbaar onder de Wdo.

Hierbij wordt opgemerkt dat wordt verwacht dat ook tijdig zorgspecifieke middelen zullen worden aangeboden. Hierover lopen momenteel gesprekken met leveranciers en koepel- en zorgorganisaties. Ook zal de voor de verplichtstelling uit het wetsvoorstel de NL-wallet beschikbaar zijn. Dit is een digitale wallet onder het EUDI-stelsel.

56

*De leden van de **BBB-fractie** willen weten hoe de regering de afhankelijkheid van commerciële leveranciers en certificerende instanties beoordeelt bij de uitvoering van een wettelijke verplichting.*

Voor de specifieke inlogmiddelen die gebaseerd zijn op de NEN 7518 is het de verwachting dat de techniek (van de inlogmiddelen) voornamelijk door commerciële partijen wordt aangeboden. Hoewel zorg- en jeugdhulpaanbieder theoretisch zelf een middel kunnen ontwikkelen of een open-source oplossing kunnen inzetten, is dit in de praktijk niet waarschijnlijk. Er is daardoor een afhankelijkheid van commerciële leveranciers op dat onderdeel.

Omdat voor het gebruik van deze zorgspecifieke middelen een officieel certificaat van een certificerende instantie vereist is, ontstaat er voor het certificeren van de NEN 7518 een rol voor commerciële leveranciers.

[35] Advies van de Afdeling advisering van de Raad van State van 24 juli 2024 (W13.24.00112/III).

Zorg- en jeugdhulpaanbieders kunnen er ook voor kiezen geen eigen zorgspecifiek middel uit te geven en in plaats daarvan middelen vanuit de Wdo in te zetten. In dat geval is er geen afhankelijkheid van een commerciële leverancier, is er geen sprake van een eis tot certificering onder de NEN 7518 en dus ook geen afhankelijkheid van een commerciële certificerende instelling.

57

*De leden van de **BBB-fractie** vragen waarom niet is gekozen voor een publieke oplossing die garant staat voor continuïteit, in plaats van afhankelijkheid van marktpartijen.*

Het wetsvoorstel biedt een grondslag voor zowel publieke als private inlogmiddelen, vanuit de kaders Wdo, PKIoverheid, de eIDAS-verordening en de NEN 7518. Juist door keuzevrijheid te bieden tussen de verschillende soorten inlogmiddelen, met een terugvaloptie naar Wdo-inlogmiddelen, wordt continuïteit van de zorgverlening gegarandeerd.

58

*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.*

Het wetsvoorstel draagt bij aan de doelstellingen van het kabinet om de zorg verder te digitaliseren. In lijn met de verdere digitaliseringsslag die het wetsvoorstel vraagt, is gekozen om uitsluitend digitaal contact met het CIBG voor te schrijven. Het CIBG biedt hierbij passende ondersteuning.

Ik heb daarbij ook meegewogen dat het aanbieden van een papieren route zou betekenen dat er een fysieke identiteitsvaststelling moet plaatsvinden op een beveiligingsniveau dat overeenkomt met de digitale route. Dit zou ook belastend zijn voor de zorg- en jeugdhulpaanbieder. Dat meegewogen, acht ik de gekozen route proportioneel.

59

*De leden van de **BBB-fractie** vragen hoe de regering de uitvoerbaarheid voor zorgaanbieders in krimpregio's, waar digitale aansluiting problematischer is en digitale systemen vaker falen beoordeelt.*

Op basis van signalen uit het veld en consultaties in de voorbereiding van het wetsvoorstel is er op dit moment geen aanleiding om te concluderen dat de uitvoerbaarheid voor zorgaanbieders in krimpregio's problematisch is.

Indien uit de pilots of signalen uit het veld blijkt dat zorg- en jeugdhulpaanbieders in krimpregio's problemen ervaren met de aansluiting op het Dezi-stelsel, zal ik bekijken welke maatregelen passend zijn.

60

*De leden van de **BBB-fractie** vragen of de regering bereid is uitzonderingen te overwegen voor partijen met beperkte ICT-capaciteit.*

Het is niet de bedoeling om generieke uitzonderingen te introduceren voor partijen met beperkte ICT-capaciteit. De betreffende verplichting maakt onderdeel uit van een bredere ontwikkeling richting verdere

digitalisering en standaardisering binnen de zorg, die noodzakelijk is voor betrouwbare en veilige gegevensuitwisseling.

Van zorg- en jeugdhulpaanbieders mag worden verwacht dat zij hun bedrijfsvoering zodanig inrichten dat zij kunnen voldoen aan wettelijke vereisten, waaronder digitale communicatie met overheidsinstanties. Dit behoort tot de normale professionele en organisatorische verantwoordelijkheid van een zorg- en jeugdhulpaanbieder.

Daarbij is het digitale proces bewust zo eenvoudig en beperkt mogelijk ingericht en geldt een overgangsperiode. Ook wordt voorzien in passende ondersteuning. Deze maatregelen zijn erop gericht om de uitvoerbaarheid te waarborgen, zonder afbreuk te doen aan het uitgangspunt dat alle communicatie door zorg- en jeugdhulpaanbieders met het CIBG digitaal plaats dient te vinden.

Vragen en opmerkingen van de leden van de SGP-fractie

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

61

*De leden van de **SGP-fractie** 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.*

Bestaande Europese en nationale kaders bieden handvatten voor strategische autonomie en nationale veiligheid. Europese inlogmiddelen die binnen het toepassingsgebied van dit wetsvoorstel worden gebruikt, moeten voldoen aan de eisen uit de eIDAS-verordening en de daarop gebaseerde toezicht- en certificeringskaders. De Wdo-middelen en het PKI-O-afsprakenstelsel staan onder toezicht van de Minister van BZK en de zorgspecifieke inlogmiddelen onder toezicht van de Inspectie Gezondheidszorg en Jeugd. Daarnaast staan de eisen van naleving van de eIDAS-verordening, waaronder de regels voor de QTSP, onder toezicht van de EU. Dit betekent dat alleen inlogmiddelen kunnen worden gebruikt die zijn erkend door de Nederlandse overheid of die onder toezicht staan van de Europese Unie. Bovendien schrijft de eIDAS-verordening voor dat een verlener van vertrouwensdiensten in de EU gevestigd hoort te zijn, een vestiging hoort te hebben in de EU of gevestigd is in een derde land dat een overeenkomst heeft gesloten met de EU op grond van artikel 218 VWEU. Ook moeten verleners van vertrouwensdiensten onder toezicht staan van een nationale toezichthouder in een EU-land.
Het kabinet onderschrijft dat het van belang is dat Nederland controle houdt over vitale digitale infrastructuur, zeker in sectoren zoals de zorg. Daarom zijn er contractueel afspraken gemaakt tussen het CIBG en private partijen over de locatie van de data en de bescherming ervan. Via een preferente aandelenconstructie is de leverancier beschermd tegen vijandige overnames, wat moet voorkomen dat de gegevens alsnog buiten de EU bewaard, ingezien of gebruikt kunnen worden. Ook zijn er aanvullende afspraken gemaakt over hoe er gehandeld dient te worden wanneer een niet-Nederlandse overheidsdienst om gegevens verzoekt. Tot slot bevat de ARBIT-2018 de
mogelijkheid tot ontbinding indien er sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van de leverancier. Bij een ontbinding kan verzocht worden om retournering van de data.

Het kabinet heeft uiteraard oog voor de actuele (geopolitieke) ontwikkelingen en de vraag of er meer nodig is om de cybersecurity op een voldoende niveau te handhaven voor de zorgsector. De plannen die ik daarvoor heb, zijn in december 2025 uiteengezet in de brief over Informatie- en Communicatietechnologie in de Zorg.[36]

Daarbij werkt het kabinet met een risico-gerichte aanpak aan onze strategische autonomie, op nationaal en Europees niveau. In het kader van digitale soevereiniteit is in december 2025 de "Visie Digitale autonomie van de overheid" vastgesteld.[37] Hierin staat de strategische richting waarmee de Nederlandse overheid haar digitale autonomie en haar digitale soevereiniteit kan versterken, onder andere door het beperken van de afhankelijkheden van niet Europese digitale aanbieders. Binnen de Nederlandse Digitaliseringsstrategie (NDS) is digitale weerbaarheid en autonomie één de prioriteiten waarop wordt ingezet.[38]

62

*De leden van de **SGP-fractie** vragen of de regering kan aangeven in hoeverre we ten aanzien van inlogmiddelen op dit moment afhankelijk zijn van niet-Europese marktpartijen.*

Op dit moment dreigt een leverancier, Solvinity, overgenomen te worden door het Amerikaanse Kyndryl. Het bedrijf Solvinity draagt zorg voor het technisch beheer van de infrastructuur, servers, updates en de performance van DigiD en andere Logius diensten. In november 2025 is de beoogde overname van Solvinity door Kyndryl aangekondigd. De voorgenomen overname wordt op dit moment getoetst door twee onafhankelijke toezichthouders. Daarnaast heeft het kabinet zelf opdracht gegeven om te kijken naar de operationele en strategische (veiligheids)risico's bij de Solvinity-casus en lopen er gesprekken met Solvinity en Kyndryl.

Onder de Wdo is het mogelijk om nieuwe inlogmiddelen toe te laten tot de Nederlandse digitale dienstverlening. Deze en bestaande inlogmiddelen, zowel publiek als privaat, zullen aan de eisen van de Wdo moeten voldoen. Deze eisen bouwen voort op de eisen uit Europese eIDAS-verordening. De huidige wet- en regelgeving stelt kaders om inlogmiddelen veilig, betrouwbaar en beschikbaar te houden. De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op het toelatingsproces en het gebruik van deze inlogmiddelen.

63

*De leden van de **SGP-fractie** vragen in bredere zin of er door de regering wordt gewerkt aan het in kaart brengen van de afhankelijkheid van niet-Europese bedrijven als het gaat om kritieke functies in de zorg.*
Er wordt niet gewerkt aan het in kaart brengen van afhankelijkheden van niet-Europese diensten. In mijn Kamerbrief over informatieveiligheid in de zorg van 4 december 2025 ben ik verder ingegaan op het belang van digitale autonomie.[39] Afhankelijkheid van leveranciers, binnen en buiten Europa, kan risico's met zich meebrengen. Ik roep de sector daarom op om in hun risicoafweging de afhankelijkheid van leveranciers mee te nemen.

De Minister van Langdurige Zorg,
Jeugd en Sport,

[36] Kamerstukken II 2025-2026, nr. 353.

[37] *Visie- Digitale autonomie en soevereiniteit van de overheid,* 30 juni 2025, link: Visie - Digitale autonomie en soevereiniteit van de overheid.

[38] De Nederlandse Digitaliseringsstrategie, juni 2025, link: De Nederlandse Digitaliseringsstrategie.

[39] Kamerstukken II, 2025-2026, 27529, nr. 353.

W.R.C. Sterk