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

Introductie

Met belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Volksgezondheid, Welzijn en Sport 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 de PVV, GroenLinks-PvdA, VVD, NSC, CDA en SP 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 verslag gekozen paragraafindeling. In deze nota zijn de vragen en opmerkingen uit het verslag integraal opgenomen in cursieve tekst en de beantwoording daarvan in gewone typografie.

Leeswijzer

In deze nota naar aanleiding van het verslag wordt de volgorde van de hoofdstukken in het verslag aangehouden.

1. Inleiding

De leden van de GroenLinks-PvdA-fractie onderstrepen het belang van een veilige identificatie en authenticatie in de zorg. Generieke functies die breed van toepassing zijn, horen gecoördineerd te worden door de overheid. Deze leden vragen wat de coördinerende taak van de minister van VWS precies inhoudt en welke mogelijkheden zij heeft om naleving van de wet af te dwingen. In het digitale domein zien zij dat standaarden, ook binnen de rijksoverheid, nog niet voldoende worden nageleefd. Waarom zal dit nu wel het geval zijn? Daarnaast vragen deze leden of de staatssecretaris voor Digitalisering en de CIO Rijk betrokken zijn bij de totstandkoming van het wetsvoorstel en zo ja, wat precies hun rol is.

Veilige en betrouwbare identificatie en authenticatie zijn randvoorwaardelijk voor digitale zorg. Aangezien dit generieke functies zijn die domein- en sector-overstijgend en nodig zijn, heb ik een coördinerende taak. Deze taak omvat het opstellen van beleidskaders, het bevorderen van standaardisatie en interoperabiliteit en het faciliteren van implementatie in alle zorgsectoren. Door de regierol die ik bekleed, wordt geborgd dat zorgpartijen veilig, efficiënt en eenduidig kunnen werken met, in dit geval, een digitale identiteit.

Het is juist dat wordt opgemerkt dat standaarden, ook binnen de rijksoverheid, in de praktijk niet altijd worden nageleefd. In eerdere trajecten, zoals bij digitale toegankelijkheid, bleek dat het ontbreken van afdwingbaarheid en toezicht leidde tot beperkte naleving. Die lessen zijn nadrukkelijk meegenomen bij de inrichting van het Dezi-stelsel, dat het UZI-stelsel zal vervangen. Dezi staat voor ‘De Zorgidentiteit’.

Wat dit wetsvoorstel anders maakt, is dat de naleving van standaarden niet optioneel is. Het gebruik van goedgekeurde inlogmiddelen en de aansluiting op het Dezi-register is wettelijk verplicht en de Inspectie Gezondheidszorg en Jeugd (IGJ) houdt toezicht op de naleving ervan. De IGJ kan handhaven wanneer instellingen zich niet aan de verplichtingen op basis van dit wetsvoorstel houden. Alleen middelen die voldoen aan de gestelde normen, zoals NEN 7518 en betrouwbaarheidsniveau hoog zoals vastgesteld in de eIDAS-verordening, worden toegelaten. De toegang (via een koppelvlak) is technisch zo ingeregeld dat het niet mogelijk is om anders in te loggen dan met deze goedgekeurde inlogmiddelen. Het gebruik van afwijkende of onvoldoende veilige oplossingen is op deze manier uitgesloten.

De staatssecretaris voor Digitalisering en het CIO Rijk zijn niet betrokken geweest bij de totstandkoming van dit wetsvoorstel. Het ontwerp van het Dezi-stelsel sluit uiteraard wel naadloos aan bij de lijn van het Ministerie van BZK op zowel het gebied van toegang als veiligheid. Er wordt op dit moment zelfs verkend of wij gezamenlijk een pilot kunnen gaan draaien met de nieuwe EU Digital Identity Wallet.[1] Dit is een digitale tool voor digitale identificatie en het delen van persoonlijke gegevens voor burgers en bedrijven. Met de EU Digital Identity Wallet kunnen belangrijke digitale documenten veilig worden opgeslagen, gedeeld en ondertekend. De EU Digital Identity Wallet wordt verwacht in november 2026.

De leden van de CDA-fractie delen het grote belang van verbeterde gegevensuitwisseling in de zorg. Voor deze leden geldt hierbij als uitgangspunt dat er, zeker in het licht van de toenemende digitale dreigingen en het toenemende belang van strategische autonomie, een belangrijke taak voor de overheid ligt om de veiligheid van patiëntgegevens en gegevens van zorgverleners te waarborgen en hierover de regie te nemen. Genoemde leden vragen of de regering dit

uitgangspunt deelt, mede in het licht van de geopolitieke ontwikkelingen. Voorts vragen zij of de regering deelt dat voorkomen moet worden dat Nederland voor wat betreft inlogmiddelen in de zorg afhankelijk is van (statelijke) actoren van buiten de Europese Unie.

De regering deelt de mening van de CDA-fractie dat er, zeker gezien de toenemende digitale dreigingen en het belang van strategische autonomie, een belangrijke taak voor de overheid ligt om de veiligheid van patiëntgegevens en de gegevens van zorgverleners te waarborgen. Om die reden kiest zij er met dit wetsvoorstel voor haar regierol op dit gebied vorm te geven.

[1] Artikel 5a 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.

Bij het voorstel is ruimschoots aandacht besteed aan het voorkomen van afhankelijkheid van (statelijke) actoren van buiten de Europese Unie wat betreft inlogmiddelen in de zorg. In dit kader is er daarom voor gekozen uitsluitend het gebruik van erkende inlogmiddelen toe te laten. Dit zijn middelen die vallen onder de Wet digitale overheid, de PKIoverheid, de eIDAS-verordening, of die voldoen aan NEN 7518. Dit zijn inlogmiddelen die erkend zijn door de Nederlandse overheid, onder toezicht staan van de Europese Unie, of zijn gecertificeerd door een certificerende instelling onder de Raad van Accreditatie. Hiermee wordt geborgd dat de controle over toegang tot medische gegevens binnen de Europese rechtsorde blijft, terwijl tegelijkertijd wordt voorkomen dat zorgaanbieders afhankelijk worden van buitenlandse, niet-Europese (statelijke) actoren. De regering deelt dan ook het uitgangspunt dat strategische autonomie en digitale soevereiniteit in de zorg essentieel zijn en geeft daar met dit wetsvoorstel gericht invulling aan.

1.1 Het wetsvoorstel in het kort

De leden van de PVV-fractie vragen aan de regering in hoeverre dit wetsvoorstel aansluit bij eerdere beleidsdoelstellingen voor digitale zorg. Welke bredere maatschappelijke of technologische ontwikkelingen maken deze wijziging nu urgent?

Dit wetsvoorstel volgt de door het kabinet ingezette lijn over digitalisering. In Onderdeel I van het Integraal Zorgakkoord (IZA) is afgesproken dat de generieke functies voor elektronische gegevensuitwisseling – waaronder identificatie en authenticatie – uiterlijk in 2025 gerealiseerd dienen te zijn, zodat deze sector-overstijgend ingezet kunnen worden. Dit wetsvoorstel vormt een essentiële stap in de uitvoering van die afspraak. Ook in het coalitieakkoord van het vorige kabinet is nadrukkelijk ingezet op standaardisering van gegevensuitwisseling in de zorg. Met de inwerkingtreding van de Wegiz is daarvoor een wettelijk kader opgezet. De Wegiz ziet namelijk toe op interoperabiliteit van elektronische gegevensuitwisseling tussen zorgverleners aan de hand van eenduidige eisen aan taal en techniek.

De manier waarop zorg wordt verleend en de organisatie ervan is de afgelopen jaren veranderd. Het huidige UZI-register sluit hier onvoldoende op aan. Er is behoefte aan een andere manier van inloggen en een meer centrale en eenduidige identificatie van zorgaanbieders en zorgmedewerkers. Hierin wordt voorzien met dit wetsvoorstel. Bovendien zorgt het wetsvoorstel voor een van de randvoorwaarden die noodzakelijk zijn voor de implementatie van de European Health Data Space Verordening (EHDS).

De behoefte aan een andere manier van inloggen is gelegen in het feit dat een verschuiving heeft plaatsgevonden naar meer ambulante en mobiele zorg. Hierdoor is behoefte ontstaan aan flexibele en mobiele persoonsgebonden inlogmiddelen. Dit is niet mogelijk binnen het UZI-register, maar kunnen wel in het Dezi-stelsel worden ontwikkeld.

Ook de organisatie van de zorg is veranderd; die vindt in toenemende mate plaats binnen zorgketens. Om de zorg binnen die ketens goed te laten aansluiten, is het noodzakelijk dat gezondheidsinformatie digitaal kan worden uitgewisseld. Een uniforme en betrouwbare toegang tot gegevens is hierbij een vereiste. De voorgestelde wetswijziging voorziet in een centrale, eenduidige identificatie van zowel zorgaanbieders als zorgmedewerkers via het Dezi-register.

De leden van de GroenLinks-PvdA-fractie lezen dat door het gebruiken van De Zorgidentiteit (Dezi) en het bijbehorende register, inloggen makkelijker, flexibeler en goedkoper wordt. Zij vragen de regering om uit te leggen hoe dit met zekerheid kan worden gezegd, als de inlogmiddelen nog niet zijn ontwikkeld. Hoe weet de regering zeker dat wetgeving deze verbeteringen daadwerkelijk realiseert?

In tegenstelling tot het gesloten karakter van het huidige stelsel, maakt dit wetsvoorstel een open model mogelijk. Hierdoor kunnen verschillende publieke én private inlogmiddelen worden gebruikt, mits zij voldoen aan het vereiste betrouwbaarheidsniveau hoog. Hiermee is een betere bescherming van persoonsgegevens mogelijk. Daarnaast maakt dit het mogelijk om een inlogmiddel te kiezen dat in het werkproces van de zorginstelling past en die zorgen voor een betere bescherming van persoonsgegevens.

Vanaf november 2026 geldt voor publieke én bepaalde private dienstverleners binnen de EU een wettelijke verplichting om een digitale wallet te accepteren: De European Digital Identity-Wallet.[2] Deze acceptatieplicht brengt naar alle waarschijnlijkheid een ontwikkeling met zich mee op de markt voor digitale identiteitsmiddelen. De verwachting is dat in aanloop naar 2026 een groeiend aanbod van

[2] Digitale Overheid, *de EDI-wallet Identiteit*.

gecertificeerde digitale wallets en bijbehorende infrastructuur ontstaat door publieke en private partijen. Deze wallets worden ook bruikbaar voor gebruik in het Dezi-stelsel.

Voorafgaand aan dit wetsvoorstel zijn meerdere proof of concepts (PoC's) en pilots uitgevoerd met nieuwe inlogmiddelen, waaronder DigiD en digitale wallets. De resultaten van de PoC's en pilots worden op dezi.nl gepubliceerd. Deelnemers gaven aan dat deze middelen eenvoudiger, sneller en beter inzetbaar zijn binnen bestaande werkprocessen, zeker in mobiele contexten zoals de thuiszorg en ambulancezorg. Deze ervaringen onderbouwen de technische en gebruikersgerichte haalbaarheid van het beoogde stelsel.

Het Dezi-register maakt het mogelijk om de zorgidentiteit centraal vast te leggen en te koppelen aan verschillende middelen. Wijzigingen in bijvoorbeeld rol, bevoegdheid of werkgever hoeven daardoor niet langer te leiden tot het uitgeven van een nieuw inlogmiddel. Dit is nu bij de UZI-pas wel het geval. Zo moet een zorgmedewerker die overstapt naar een andere organisatie een nieuwe UZI-pas aanvragen en betalen. Hiervoor moet deze fysiek aanwezig zijn om de pas van een koerier in ontvangst te nemen. Dit maakt het proces omslachtig en tijdrovend. Ook bij verlies of diefstal moet een nieuwe aanvraag worden gedaan, wat opnieuw kosten betekent en doorlooptijd vraagt.

Het huidige systeem kent verder aanzienlijke kosten per UZI-pas (€255 per medewerker, elke 3 jaar exclusief beheerkosten). In het nieuwe stelsel ontstaat ruimte voor concurrentie op prijs. Dit maakt het stelsel beter schaalbaar en goedkoper in het gebruik. Uit een voorlopig kostenanalyse door KPMG volgt dat de kosten per gebruiker lager zijn. Zie hiervoor ook paragraaf 10.2 van de memorie van toelichting. Dit rapport wordt binnenkort gepubliceerd op rijksoverheid.nl.

De leden van de VVD-fractie lezen dat de in het register ingeschrevenen gemakshalve aangeduid worden als zorg- en jeugdhulpaanbieders en hun medewerkers. Wat de indruk wekt dat het voorstel geldt voor alle medewerkers van een zorgaanbieder, ook de medewerkers die niet in direct contact staan met de patiënten. Deze leden vragen of dit klopt en zo nee, of het begrip medewerker nader gedefinieerd kan worden.

Het wetsvoorstel ziet toe op zorgaanbieders, zorgmedewerkers, zorgverzekeraars, indicatieorganen jeugdhulpaanbieders, jeugdhulpverleners en medewerkers die werkzaamheden verrichten of gaan verrichten voor jeugdhulpaanbieders. In verband met de leesbaarheid van de memorie van toelichting bij het wetsvoorstel is ervoor gekozen om deze in organisaties en personen in de tekst aan te duiden als "zorg- en jeugdhulpaanbieders en hun medewerkers." Hierbij is ook het begrip 'medewerker' nader gespecificeerd, namelijk: natuurlijke personen die werkzaamheden verrichten of gaan verrichten voor zorgaanbieders, jeugdhulpaanbieders, indicatieorganen en zorgverzekeraars en daarbij cliëntgegevens verwerken.

Het wetsvoorstel is kortom niet van toepassing op alle medewerkers van zorg- en jeugdhulpaanbieders, maar uitsluitend op die medewerkers die beroepsmatig zorg verlenen of in het kader van hun functie werkzaam zijn of zullen zijn in de zorg of jeugdhulp én daarbij cliëntgegevens verwerken. Gezien het feit dat deze medewerkers cliëntgegevens mogen verwerken, is identificatie en authenticatie nodig op het vereiste betrouwbaarheidsniveau hoog.

De leden van de SP-fractie vragen of de regering uitgebreider kan toelichten tot welke gegevens zorgverleners toegang kunnen krijgen via de beoogde toepassingen voor identificatie en authenticatie. Gaat het hier uitsluitend om het toegang krijgen tot het burgerservicenummer (hierna: BSN) of gaat het hierbij om een bredere set aan persoonsgegevens?

Zorgmedewerkers die door de zorgaanbieder toegang hebben gekregen tot de Sectorale Berichten Voorziening – Zorg (SBV-Z), krijgen nadat zij via de SBV-Z zijn ingelogd op de Beheervoorziening burgerservicenummer (BV-BSN) toegang tot de volgende persoonsgegevens: naam, adres, geboortegegevens, geslacht, nationaliteit, buitenlands persoonsnummer, overlijdensgegevens en het burgerservicenummer van cliënten en patiënten.

Ook kan een zorgmedewerker toegang verkrijgen tot het door de zorgaanbieder gebruikte zorginformatiesysteem en uitwisselingssysteem. Welke gegevens inzichtelijk zijn, is afhankelijk van de door de zorgaanbieder toegekende specifieke autorisatie aan de desbetreffende zorgmedewerker en

vanzelfsprekend over welke gegevens desbetreffende aanbieder beschikt. Dit zal dus maatwerk zijn per (categorie) zorgmedewerker.

1.2 Digitalisering in de zorg en het belang van identificatie en authenticatie

De leden van de GroenLinks-PvdA-fractie geven aan dat in de toelichting het belang van de patiënt onderbelicht is. Zij vragen om te onderbouwen wat de voordelen van de nieuwe wetgeving is voor patiënten, en hoe de regering zorgt dat de nieuwe inlogmiddelen bijdragen aan het vertrouwen dat patiënten hebben in de digitaliserende zorg.

De voordelen voor patiënten liggen vooral op het vlak van vertrouwen en bescherming van hun persoonsgegevens. De toegang tot de systemen is immers uitsluitend mogelijk door middel van veilige, persoonsgebonden inlogmiddelen op betrouwbaarheidsniveau hoog. Deze inlogmiddelen zijn voorbehouden aan zorgmedewerkers met de juiste autorisaties. Op deze manier wordt gewaarborgd dat alleen bevoegde professionals medische gegevens kunnen inzien.

Dit draagt bij aan het vertrouwen van patiënten in de zorgsector en in de verdere digitalisering van de zorgsector. Patiënten mogen erop rekenen dat hun gegevens zorgvuldig worden behandeld – dit wetsvoorstel versterkt die basis. Dezi zorgt ervoor dat iedereen op dezelfde manier inlogt. Dat maakt het makkelijker en veiliger om gegevens met elkaar te delen. Dit is van belang omdat in de zorg steeds vaker binnen ketens wordt gewerkt en gegevensuitwisseling dan leidt tot een actueler en meer integraal beeld over een cliënt.

De leden van de GroenLinks-PvdA-fractie zijn bovendien benieuwd tot welke patiëntgegevens zorgverleners toegang krijgen nadat zij veilig zijn ingelogd. Kan een overzicht worden gegeven van de soorten gegevens die alleen met het gebruik van inlogmiddelen voor zorgverleners te raadplegen zijn?

Zorgmedewerkers die door de zorgaanbieder toegang hebben gekregen tot SBV-Z krijgen nadat zij via de SBV-Z zijn ingelogd op de BV-BSN toegang tot de volgende persoonsgegevens: naam, adres, geboortegegevens, geslacht, nationaliteit, buitenlands persoonsnummer, overlijdensgegevens en het burgerservicenummer van cliënten en patiënten.

Ook kan een zorgmedewerker toegang verkrijgen tot het door de zorgaanbieder gebruikte zorginformatiesysteem en uitwisselingssysteem. Welke gegevens inzichtelijk zijn, hangt af van de door de zorgaanbieder toegekende autorisatie en over welke gegevens de desbetreffende aanbieder beschikt.

1.3 Het huidige UZI-register en de inlogmiddelen

De leden van de GroenLinks-PvdA-fractie vinden het bittere noodzaak dat alle sectoren werken aan hun cyberveiligheid. Wel vragen zij om de analyse dat het huidige UZI-register onveilig is nader te onderbouwen. Welke reële cyberveiligheidsrisico's bestaan of ontstaan er door dit register in gebruik te houden? Hoe vaak hebben er datalekkages plaatsgevonden in het (gebruik van het) UZI-register en door de bijbehorende inlogmiddelen?

Het huidige UZI-register voldoet aan de normen voor Public Key Infrastructure voor de overheid (PKIo) en is door de Rijksinspectie Digitale Infrastructuur erkend als gekwalificeerde vertrouwensdienst onder de eIDAS-verordening. Hierdoor is het CIBG een gekwalificeerde verlener van vertrouwensdiensten (*Qualified Trust Service Provider*) en mag het certificaten afgeven die hoogwaardig en betrouwbaar zijn. Momenteel zijn dit de UZI-middelen. Door het voldoen aan deze diverse internationale standaarden, waarop jaarlijks geaudit wordt, is het UZI-register veilig.

Door het huidige niveau van automatisering van het UZI-register is het technisch niet mogelijk om aan te sluiten op de Basisregistratie Personen. Dit heeft te maken met een verschil in gehanteerde standaarden. Hierdoor kunnen adresgegevens ongemerkt verouderd zijn. Deze technische onmogelijkheid heeft in 2024 tot 11 gemelde datalekken geleid en in 2025 tot dusver 10 datalekken. Dit betrof met name brieven waarin geregistreerden werden herinnerd aan het verlengen van hun UZI-middel, welke dus naar een onjuist adres zijn verzonden. De ontvanger kan in zo'n geval overigens enkel kennis nemen van de gegevens in de brief. De brief bevat geen bijzondere persoonsgegevens en er ontstaat geen mogelijkheid om onbevoegd een pas aan te vragen. Dit soort datalekken zullen onder het Dezi-stelsel niet meer voorkomen, omdat alle correspondentie digitaal plaats zal vinden.

De leden van de GroenLinks-PvdA-fractie begrijpen de verwijzing naar de Europese eIDAS-Verordening. Zij vragen de regering om helder uit te leggen wat de technische eisen zijn van een 'hoog' betrouwbaarheidsniveau. Ook zijn ze benieuwd naar de toekomstbestendigheid van de verordening.

In Uitvoeringsverordening (EU) 2015/1502 staan de minimale technische specificaties, normen en procedures voor het voldoen aan betrouwbaarheidsniveau laag, substantieel en hoog.[3] Deze verordening werkt een onderdeel van de eIDAS-verordening verder uit.[4] Met betrekking tot het beoogde betrouwbaarheidsniveau voor dit wetsvoorstel, zijn de eisen voor identificatie en authenticatie van belang.

Voor identificatie moet aan verschillende technische elementen voldoen om het betrouwbaarheidsniveau hoog te behalen, zoals het in bezit zijn van een erkend identiteitsbewijs voorzien van een foto of biometrische gegeven en het kunnen verifiëren dat een persoon in bezit is van een dergelijk bewijs door het te vergelijken met één of meer fysieke kenmerken van de persoon met een gezaghebbende bron.

Technische specificaties voor het betrouwbaarheidsniveau hoog voor authenticatie zijn onder andere dat een authenticatiemechanisme voorziet in beveiligingscontroles voor het verifiëren van elektronische identificatiemiddelen en die het zeer onwaarschijnlijk maken dat authenticatie-mechanismen kunnen worden omzeild door methodes als gissen, afluisteren, her-afspelen of manipulatie van communicatie.

De vereisten die de eIDAS-verordening oplegt zijn technologie-neutraal. Het moet volgens de verordening mogelijk zijn het vereiste betrouwbaarheidsniveau te bereiken met verschillende technologieën.[5] Daarmee is de eIDAS-verordening toekomstbestendig, ook in een tijd dat technologische ontwikkelingen steeds sneller gaan.

De leden van de GroenLinks-PvdA-fractie vragen hoe de regering met dit wetsvoorstel anticipeert op nieuwe en veiligere standaarden.

Het wetsvoorstel noemt geen vaste technische eisen voor inlogmiddelen, maar verwijst naar de Wet digitale overheid, PKIoverheid, de eIDAS-verordening en de NEN 7518. Hierdoor is er ruimte mee te bewegen met technologische ontwikkelingen. In deze kaders staat namelijk aan welke normen voldaan moet worden om een bepaald betrouwbaarheidsniveau te bereiken zonder dat zij precies voorschrijven hóe dit technisch moet worden uitgevoerd.

Normen evolueren mee met de praktijk en worden regelmatig herzien. Dit zorgt ervoor dat nieuwe technische inzichten en mogelijkheden kunnen worden toegepast. De eIDAS-verordening verwijst naar technische normen, zoals die van ETSI, en stelt dat passende beveiligingsmaatregelen moeten worden genomen.[6] Dit betekent dat de gebruikte technieken en standaarden steeds actueel en passend moeten zijn bij de stand van de techniek.

De leden van de GroenLinks-PvdA-fractie vragen of het wetsvoorstel digitale identificatie en authenticatie in de zorg de regering de mogelijkheid geeft om de standaarden voor loginmiddelen aan te scherpen zodra er nieuwe mogelijkheden zijn.

Voor de inlogmiddelen is het betrouwbaarheidsniveau hoog vereist, zodat alleen leveranciers van vertrouwensdiensten inlogmiddelen kunnen leveren die bruikbaar zijn binnen het nieuwe stelsel. Deze leveranciers van vertrouwensdiensten moeten op grond van artikel 19 van de eIDAS-verordening passende

---

[3] 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), overweging 2.

[4] 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 2014,* L257/73).

[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 (*PbEU 2014,* L257/73).

[6] Overwegingen 72 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). Het Europees Telecommunicatie en Standaardisatie Instituut (ETSI) is een non-profitorganisatie die standaarden opstelt op het gebied van telecommunicatie in de EU.

technische en organisatorische maatregelen treffen om de risico's in verband met de veiligheid van de door hen verleende vertrouwensdiensten te beheren.

Dit betekent niet alleen dat uitsluitend middelen worden erkend die gebruikmaken van actuele technieken en standaarden, maar ook dat daarmee nieuwe standaarden zullen volgen en dat deze zullen moeten inspelen op de meest recente technologische ontwikkelingen.

2. Hoofdlijnen van het voorstel

2.1 Probleembeschrijving

De leden van de PVV-fractie vragen welke concrete problemen met dit voorstel worden opgelost, en of er alternatieve oplossingen zijn overwogen.

Het wetsvoorstel gaat een stap verder in het nog beter beschermen van gezondheidsgegevens van patiënten en cliënten en het verbeteren van de uitwisseling van gegevens. Veel inlogmiddelen die momenteel in de zorg worden gebruikt, voldoen niet aan het betrouwbaarheidsniveau hoog. Dit betekent voor de patiënt dat bescherming tegen onrechtmatige toegang tot de patiëntgegevens onvoldoende is geregeld. Daarnaast spelen er andere verschillende problemen. Zo sluiten de huidige UZI-middelen niet goed aan op alle zorgprocessen. Ze werken bijvoorbeeld niet goed bij ambulant werk of op mobiele apparaten. Daarnaast worden UZI-middelen als duur ervaren. Verder zijn UZI-middelen niet flexibel. Een voorbeeld hiervan is dat bij een verandering in de werkrelatie of in de beroepsbevoegdheid een nieuw middel moet worden aangeschaft.

Dit wetsvoorstel biedt naast een oplossing voor de bovengenoemde problemen, een betere bescherming van patiëntgegevens, een verbetering van de identificatie van zorgmedewerkers, en waarborgt het recht van patiënten en cliënten van artikel 15e van de Wet cliëntenrechten bij elektronische gegevensverwerking in de zorg om te weten wie hun medische gegevens heeft ingezien.

Er is gekeken naar alternatieve oplossingsrichtingen. Een onderzocht alternatief was of het mogelijk en wenselijk is om binnen Dezi alleen gebruik te maken van het publieke inlogmiddel DigiD. Uit dat onderzoek bleek echter dat dit niet voldoende was en dat DigiD een aantal beperkingen kent. Zo kan DigiD niet gebruikt worden voor fysieke toegang, zoals het openen van deuren, en biedt het geen mogelijkheid om een zorgmedewerker te herkennen aan de hand van een foto-wat soms belangrijk is voor patiënten. Daarnaast bestaat er een risico als alles afhankelijk zou zijn van één systeem. Als DigiD tijdelijk niet werkt, bijvoorbeeld door een storing of een cyberaanval, dan zouden zorgmedewerkers mogelijk geen toegang meer hebben tot belangrijke systemen met patiëntgegevens of ruimtes. Dat is onacceptabel omdat het de continuïteit van de zorg ernstig verstoort. Daarom is het beter om meerdere betrouwbare inlogmiddelen als alternatieven naast elkaar beschikbaar te hebben. Zo blijft de zorg ook toegankelijk als één middel uitvalt en ontstaat er een veiliger en stabieler systeem.

Een ander onderzocht alternatief is dat de overheid zelf nieuwe inlogmiddelen zou gaan ontwikkelen om de huidige UZI-middelen te vervangen. Voor dit alternatief is niet gekozen, omdat er reeds andere middelen op de markt zijn of worden ontwikkeld die gebruikt kunnen worden in de zorg. Hierbij kan gedacht worden aan combinaties van DigiD met zorgspecifieke inlogmiddelen die momenteel worden ontwikkeld. Aangezien er al andere geschikte inlogmiddelen zijn en er naar verwachting nieuwe zorgspecifieke middelen bijkomen, is het niet nodig dat de overheid nieuwe eigen middelen ontwikkelt.

De leden van de GroenLinks-PvdA-fractie (h)erkennen de problemen die worden geschetst rondom de huidige identificatie en authenticatie. Zij vragen de regering om met cijfers te onderbouwen welk aandeel van de zorg- en jeugdhulpsector momenteel met het hoogste betrouwbaarheidsniveau zichzelf identificeert.

Op dit moment is het alleen mogelijk om met de UZI-pas in te loggen op betrouwbaarheidsniveau hoog. Het aantal medewerkers in de zorg- en jeugdhulpsector in bezit van een UZI-pas, en dus opgenomen zijn in het UZI-register, bedraagt op dit moment ongeveer 90.000.

De leden van de GroenLinks-PvdA-fractie vragen of kan worden geschetst hoe het komt dat identificatie en authenticatie momenteel gefragmenteerd is. Hoe kan het dat er zo'n lappendeken aan inlogmiddelen is ontstaan dat dit de kwaliteit van de zorg belemmert?

De huidige fragmentatie in identificatie- en authenticatieoplossingen in de zorg komt door de jarenlang ontbreken van centrale sturing en uniforme kaders. In die context hebben zorgaanbieders noodgedwongen gekozen voor uiteenlopende, lokaal of sectoraal passende inlogmiddelen, vaak toegespitst op specifieke systemen of werkprocessen. Het resultaat is een 'lappendeken' aan oplossingen, waarbij zorgverleners meerdere middelen naast elkaar moeten gebruiken, afhankelijk van toepassing of instelling.

Deze versnippering belemmert de kwaliteit van zorg. Het leidt tot vertraging of belemmering van veilige en tijdige toegang tot relevante gegevens, vergroot de kans op fouten en verhoogt de administratieve belasting voor zorgprofessionals. Daarnaast ondermijnt dit het vertrouwen in digitale gegevensuitwisseling, terwijl juist interoperabiliteit, betrouwbaarheid en een gebruiksvriendelijke toegang van belang zijn voor goede, samenhangende zorg.

De leden van de GroenLinks-PvdA-fractie waarderen de inzet op de interoperabiliteit van systemen. Zij pleiten ervoor om interoperabiliteit op zo veel mogelijk plekken in de digitaliserende zorg als standaard te hanteren. Welke andere mogelijkheden ziet de regering hiertoe, ook in bestaande en aanstaande wetgeving?

Ik onderschrijf het belang van interoperabiliteit als standaardprincipe binnen het digitaliseren van de zorg. Naast het voorliggende wetsvoorstel worden ook op andere vlakken maatregelen genomen, zoals bij de implementatie van de EHDS. Deze verordening vereist immers aanvullende verplichtingen voor het door de zorgaanbieder interoperabel beschikbaar stellen van elektronische gezondheidsgegevens aan andere behandelende zorgaanbieders voor kwalitatief goede, toegankelijke en betaalbare zorg aan patiënten.

De leden van de GroenLinks-PvdA-fractie onderstrepen het probleem met de betaalbaarheid van UZI-passen. Terwijl de (jeugd)zorg financieel onder druk staat, moeten zorgverleners zich niet bekommeren om de prijs van inlogmiddelen. Wanneer zijn de kosten voor dergelijke inlogmiddelen volgens de regering acceptabel en wie zou deze kosten moeten betalen?

Ik deel de zorgen over de betaalbaarheid van de huidige UZI-middelen. De kosten van €255 per pas, elke drie jaar, worden zorgbreed als hoog ervaren, zeker in sectoren waar marges beperkt zijn. De nieuwe systematiek maakt het mogelijk om gebruik te maken van meerdere goedgekeurde middelen, waaronder bestaande zorgspecifieke passen en mobiele oplossingen, mits zij voldoen aan het betrouwbaarheidsniveau hoog. Dit leidt tot keuzevrijheid, concurrentie en naar verwachting lagere kosten per gebruiker. Wat acceptabele kosten zijn is niet aan de regering om te bepalen, maar aan de zorgaanbieders.

Vanaf november 2026 is de EU Digital Identity Wallet beschikbaar.[7] Dit een gratis wallet voor alle burgers, en dus ook voor de zorgmedewerkers. Het is een digitale tool voor digitale identificatie en het delen van persoonlijke gegevens voor burgers en bedrijven. Elke lidstaat gaat minstens één wallet beschikbaar stellen aan al haar burgers, inwoners en bedrijven, zodat ze kunnen bewijzen wie ze zijn en belangrijke digitale documenten veilig kunnen opslaan, delen en ondertekenen. In een wallet kunnen Verklaringen worden geladen. Deze Verklaringen zijn daarbij het bewijs van de zorgidentiteit van de zorgmedewerker. De wallet wordt daarmee ook geschikt om mee in te loggen via Dezi.

Het wordt wenselijk geacht dat de kosten voor inlogmiddelen primair op zorgaanbiederniveau worden belegd en niet bij de individuele zorgmedewerkers. Bij de implementatie zal nadrukkelijk aandacht zijn voor de betaalbaarheid, met oog voor schaalgrootte. Het wetsvoorstel biedt in ieder geval de ruimte om de kosten omlaag te brengen door marktwerking en hergebruik van bestaande middelen.

Tegelijkertijd brengt dit wetsvoorstel met zich mee dat er minder vaak middelen aangeschaft hoeven te worden. Dat heeft een kostendrukkend effect: er hoeft immers niet steeds een nieuw middel te worden aangeschaft wanneer een medewerker bij een andere zorgaanbieder gaat werken, een andere functie krijgt of een middel verliest.

De leden van de GroenLinks-PvdA-fractie zijn benieuwd of en hoe vaak het voorkomt dat medewerkers UZI-passen onderling uitlenen. Waarop baseert de regering deze aanname? Hoe vaak komt dit naar schatting voor?

[7] Artikel 5a 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.

Het is niet mogelijk om inzichtelijk te maken hoe vaak een middel wordt uitgeleend. In gesprekken met zorgaanbieders wordt echter aangegeven dat het voorkomt. Als er gebruik wordt gemaakt van een inlogmiddel uit het Dezi-stelsel dan is er een hogere drempel om het persoonlijke inlogmiddel uit te lenen, bijvoorbeeld als voor het inloggen gebruik wordt gemaakt van een telefoon.

De leden van de NSC-fractie begrijpen dat het nieuwe Dezi-register alleen verplicht zal worden gesteld voor de Sectorale Berichten Voorziening in de Zorg (SBV-Z). Tegelijkertijd oordeelde de Raad van State dat met een beperkte mate van verplichting het nieuwe register ook beperkt effect zal hebben. Genoemde leden vragen de regering waarom er is gekozen voor vrijwillige deelname aan het register behalve voor de SBV-Z. Hoe wordt voorkomen dat zorgorganisaties oude en veelal minder veilige inlogsystemen behouden?

Het beeld dat deelname aan het Dezi-register uitsluitend verplicht zou worden voor toegang tot de SBV-Z is onjuist. Dit was wel het geval voordat de Afdeling advisering van de Raad van State over het wetsvoorstel adviseerde. Naar aanleiding van het advies is het wetsvoorstel aangepast en voorziet het nu in een wettelijke basis om het gebruik van het Dezi-register en inlogmiddelen op betrouwbaarheidsniveau hoog ook verplicht te stellen voor toegang tot elektronische uitwisselingssystemen als zorginformatiesystemen.

Door deze verplichting wordt voorkomen dat zorgorganisaties oude en veelal minder veilige inlogsystemen behouden, omdat voor toegang tot zowel elektronische uitwisselingssystemen als zorginformatiesystemen Dezi gebruikt moet worden. Andere inlogmiddelen zullen dan geen toegang meer kunnen geven. De IGJ zal hierop toezicht houden.

2.2 Doelstelling en noodzaak wetgeving

De leden van de PVV-fractie vragen waarom wetgeving noodzakelijk is, in plaats van bijvoorbeeld brancheafspraken.

De regering kiest bewust voor wettelijke verankering van het Dezi-stelsel en niet voor brancheafspraken of vrijwillige convenanten. Allereerst vereist de verwerking van het BSN een expliciete wettelijke grondslag. Branche-afspraken bieden die grondslag niet. Daarnaast is wetgeving noodzakelijk om landelijke uniformiteit, sector-overstijgende toepassing en handhaafbaarheid te waarborgen. Alleen met een wettelijk kader kan worden voorkomen dat versnippering in identificatie- en authenticatiemethoden de voortgang van digitale gegevensuitwisseling belemmert en kan hierop toezicht worden gehouden. Met branche-afspraken kan dit niet worden bereikt. Wetgeving biedt daarom de noodzakelijke juridische en maatschappelijke borging van veilige digitale toegang in de zorg.

De leden van de GroenLinks-PvdA-fractie herkennen nogmaals de probleemstelling over het niet van de grond komen van generieke functies. Echter is het stellen van de juiste standaarden nog geen garantie dat deze worden nageleefd, zolang ze geen dwingend karakter hebben. Zij verwijzen naar de overheid die massaal de eigen toegankelijkheidseisen voor websites en digitale formulieren niet naleeft. Waarom is wetgeving volgens de regering nu wel effectief om te komen tot landelijke standaarden voor generieke functies?

De regering onderkent dat het vaststellen van standaarden op zichzelf onvoldoende zijn om naleving te garanderen. Daarom voorziet het wetsvoorstel in een juridisch bindende verplichting tot aansluiting op het Dezi-register en het gebruik van goedgekeurde inlogmiddelen op betrouwbaarheidsniveau hoog. Als daar niet aan wordt voldaan, kan er niet worden ingelogd in het Dezi-register. Voorts kan de IGJ zo nodig handhavend optreden, indien deelname door zorgaanbieders uitblijft, of als zij niet aan de gestelde eisen voldoen. Hierin wordt voorzien middels een nota van wijzing op dit wetsvoorstel. De combinatie van wetgeving, technische borging, gecombineerd met ondersteuning bij standaardisatie-inspanningen en toezicht en handhaving, maken de aanpak van dit wetsvoorstel wezenlijk effectiever dan eerdere vrijwillige standaardisatie-inspanningen zoals bij digitale toegankelijkheid. Deze totaalaanpak is noodzakelijk om te komen tot een toekomst-vast en robuust stelsel.

De leden van de GroenLinks-PvdA-fractie begrijpen waarom er andere middelen moeten komen voor veilige identificatie en authenticatie. Echter vragen zij om nader uit te leggen waarom het niet wenselijk is dat inlogmiddelen door de minister van VWS (via het CIBG) worden uitgegeven. Waarom is er niet voor gekozen om, naast de mogelijkheid te bieden voor nieuwe betrouwbare inlogmiddelen, ook een eigen (open source) inlogmiddel van een hoog betrouwbaarheidsniveau te ontwikkelen als terugvaloptie? Lekt er door de verschuiving naar externe inlogmiddelen geen technische expertise weg uit het ministerie van VWS?

Het wetsvoorstel maakt het mogelijk om DigiD te gebruiken als een publiek inlogmiddel voor de toegang tot zorginformatie- en gegevensuitwisselingssystemen. DigiD kan door een zorgmedewerker dagelijks worden gebruikt als inlogmiddel, of enkel als terugvaloptie worden ingezet. Het DigiD-inlogmiddel kan ook gebruikt worden voor authenticatie op het betrouwbaarheidsniveau hoog. Naast het publieke DigiD-inlogmiddel kunnen ook (erkende) marktmiddelen worden gebruikt. Als het Ministerie van VWS naast DigiD nog een ander publiek inlogmiddel (open source) laat ontwikkelen, zal dit de markt verstoren voor de (private) leveranciers van inlogmiddelen binnen het Dezi-stelsel. Dit zou ook het doel van het Dezi-stelsel, dat een multi-middelenstelsel beoogt met keuzevrijheid, innovatie en alternatieven/terugvalopties, in de weg staan. Het doel is om meerdere inlogmiddelen beschikbaar te maken die door verschillende partijen op de markt worden aangeboden. Dit biedt het beste antwoord voor vragen over betaalbaarheid, gemak in het gebruik, aansluiting bij wat de zorg nodig heeft en veiligheid.

Voor het Dezi-stelsel wordt de benodigde technische expertise en kennis over inlogmiddelen geborgd binnen het CIBG, op dezelfde manier als bij het huidige UZI-register. Dit gebeurt door het inzetten van een gespecialiseerd team binnen het CIBG dat verantwoordelijk is voor beheer, ondersteuning en doorontwikkeling, waarbij gebruik wordt gemaakt van bestaande infrastructuur en ervaring.

De leden van de VVD-fractie lezen dat door het niet langer vanuit de overheid aanbieden van middelen er ruimte ontstaat voor verschillende partijen om diverse inlogmiddelen te ontwikkelen. Genoemde leden vragen of de regering partijen zal aanwijzen of dat partijen zich hiervoor kunnen inschrijven. Daarnaast de vraag of aan een maximumaantal partijen wordt gedacht.

De regering gaat geen specifieke partijen aanwijzen om de genoemde diverse inlogmiddelen te ontwikkelen. De reden daarvoor is, dat dit wetsvoorstel bepaalt dat inlogmiddelen kunnen worden erkend indien zij aan de betreffende, bij dit wetsvoorstel aangegeven, eisen voldoen.

Deze eisen worden gesteld binnen de kaders van de Wet digitale overheid, NEN-7518, PKIoverheid en de eIDAS-verordening. Als aan de eisen uit een van deze kaders wordt voldaan, wordt een inlogmiddel als betrouwbaar beschouwd (betrouwbaarheidsniveau hoog). Er zijn dus meerdere kaders met eisen waaraan een inlogmiddel kan voldoen. Om erkend te worden, moet er een aanvraag worden gedaan bij het CIBG. Het CIBG keurt vervolgens een inlogmiddel voor het Dezi-stelsel goed. Aangezien het hier gaat om kwalitatieve vereisten is er geen maximumaantal van aanbieders voor inlogmiddelen voorzien.

De leden van de VVD-fractie merken op dat de gekozen oplossingsrichting is afgestemd met het zorgveld en zij vragen in hoeverre de eindgebruikers, dus de zorgprofessionals, onderdeel zijn geweest van deze afstemming. In hoeverre is de paramedische sector betrokken bij de afstemming?

De gekozen oplossing is ontwikkeld in samenwerking met het zorgveld. Het Ministerie van VWS heeft, mede via Nictiz, de afgelopen jaren informatie, behoeften en kennis verzameld van zorginstellingen, zorgkoepels en leveranciers. Er zijn bezoeken gebracht aan verschillende zorginstellingen waar gesprekken zijn gevoerd met zorgverleners, architecten, (informatie-) managers en *Chief Medical Information Officers*. De visie van zorgkoepels over dit werkveld is actief opgehaald. Ook zijn er expertsessies georganiseerd over verschillende inhoudelijke onderwerpen, waarbij zorgmedewerkers betrokken waren. De oplossingsrichting is gedeeld en besproken met het zorgveld via online seminars, vragenuurtjes, beurzen/congressen, nieuwsbrieven, de CIBG-website en systeemdocumentatie. Daarnaast is een klankbordgroep opgericht, waar zorgkoepels en VZVZ deel van uitmaken.

Om gebruikerservaring op te doen, zijn er pilots uitgevoerd. Dit gebeurde door zorgverleners te laten testen met de oplossing die via dit wetsvoorstel mogelijk wordt gemaakt. Zo konden zorgmedewerkers inloggen met het inlogmiddel DigiD en een ID-wallet van Yivi en is hun gebruikerservaring meegenomen.[8]

De paramedische sector is in de klankbordgroep niet vertegenwoordigd en ook niet direct via andere overleggen en/of gremia.

Eenieder die niet rechtstreeks is benaderd of in het voorproces betrokken is geweest, heeft via de internetconsultatie inbreng kunnen leveren op dit wetsvoorstel. Vanuit de paramedische sector is door de

[8] Data voor Gezondheid, *'VWS start pilot met wallet als alternatief voor UZI-pas'*.

KNGF (Fysiotherapeuten) gereageerd bij de internetconsultatie, evenals onder andere de NVZ (ziekenhuizen), V&VN (Verpleegkundigen & Verzorgenden) en de LHV (huisartsen).

De leden van de VVD-fractie vragen naar het gebruik van DigiD. In maart 2025 was DigiD tijdelijk onbereikbaar door een DDoS-aanval (distributed denial-of-service) en dit gebeurt helaas vaker. Op welke wijze wordt het onbereikbaar zijn van inlogmiddelen door dergelijke aanvallen opgevangen?

Het onbereikbaar zijn van inlogmiddelen kan niet volledig worden voorkomen. Wel zijn er twee maatregelen getroffen in het wetsvoorstel die deze risico's verkleinen. Ten eerste verplicht het wetsvoorstel dat zorgaanbieders en zorgmedewerkers met verschillende goedgekeurde inlogmiddelen kunnen inloggen. Hierdoor is er toegang tot elektronische uitwisselingssystemen of zorginformatiesystemen mogelijk met andere goedgekeurde inlogmiddelen.

Ten tweede ontstaan er met de komst van identiteitswallet nieuwe type inlogmiddelen die, net als PKIo-middelen, minder afhankelijk zijn van centrale componenten. Hierdoor heeft een DDoS-aanval minder of geen invloed heeft op deze middelen. Als het inlogmiddel DigiD, een van de erkende Dezi-middelen, niet beschikbaar is, kan een zorgmedewerker een alternatief middel gebruiken dat ook bruikbaar is binnen het Dezi-stelsel. Het Dezi-stelsel biedt dus alternatieven die als terugvaloptie gebruik kunnen worden. Daarnaast wordt vanaf november 2026 voor iedere EU-burger ten minste één (gratis) European Digital Identity-wallet beschikbaar. Deze wallets hebben bij gebruik een beperkte afhankelijkheid van centrale componenten. De zorgidentiteit van de zorgmedewerker wordt namelijk vooraf, op verzoek van de zorgmedewerker, door het CIBG als een
'verklaring' in de wallet wordt geplaatst. Deze verklaring kan direct bij de zorgaanbieder worden aangeboden. Hierdoor heeft een DDoS-aanval op een centrale voorziening zoals DigiD geen of veel minder grip heeft op dit soort inlogmiddelen.

De leden van de NSC-fractie achten het van groot belang dat de werkvloer voldoende betrokken is bij het ontwerp van het nieuwe stelsel. Op welke wijze zijn zorgprofessionals meegenomen in het ontwerp van het nieuwe register en de keuze voor de inlogmiddelen? Wat was de feedback van zorgprofessionals op het ontwerp?

De gekozen oplossing is in samenwerking met het zorgveld ontwikkeld. Het Ministerie van VWS heeft, mede via Nictiz, de afgelopen jaren informatie, behoeften en kennis verzameld van zorginstellingen, zorgkoepels en leveranciers. Er zijn bezoeken gebracht aan verschillende zorginstellingen, waar gesprekken werden gevoerd met zorgverleners, architecten, (informatie-) managers en *Chief Medical Information Officers.* De visie van zorgkoepels over dit werkveld is actief opgehaald. Ook zijn er expertsessies georganiseerd over verschillende inhoudelijke onderwerpen, waarbij zorgmedewerkers betrokken waren. De oplossingsrichting is gedeeld en besproken met het zorgveld via: online seminars, vragenuurtjes, beurzen/congressen, nieuwsbrieven, de CIBG-website en systeemdocumentatie. Daarnaast is een klankbordgroep opgericht, waar zorgkoepels en VZVZ deel van uitmaken. Eenieder die niet rechtstreeks is benaderd of in het voorproces betrokken is geweest, heeft via de internetconsultatie inbreng kunnen leveren op dit wetsvoorstel. Vanuit de paramedische sector is door de KNGF (Fysiotherapeuten) bij de internetconsultatie gereageerd, evenals onder andere de NVZ (ziekenhuizen), V&VN (Verpleegkundigen & Verzorgenden) en de LHV (huisartsen).

Om gebruikerservaring op te doen, zijn er pilots uitgevoerd. Dit gebeurde door zorgmedewerkers te laten testen met de oplossing die via dit wetsvoorstel mogelijk wordt gemaakt. Zo konden zorgmedewerkers inloggen met het inlogmiddel DigiD en met een ID-wallet van Yivi en is hun gebruikerservaring meegenomen.

Een belangrijk onderdeel van deze oplossing is dat zorgmedewerkers zelf kunnen kiezen welk Dezi-inlogmiddel ze gebruiken. Deze keuzevrijheid wordt erg gewaardeerd door de zorgmedewerkers. Daarnaast waarderen zorgmedewerkers dat elk erkend inlogmiddel bij elke zorgaanbieder werkt. Hierdoor hoeft een zorgmedewerker niet meerdere inlogmiddelen te hebben als hij of zij bij verschillende zorgorganisaties werkt.

De leden van de NSC-fractie lezen in het advies van de Raad van State dat zonder een harde einddatum voor het verplicht overstappen naar het Dezi-register, het nieuwe stelsel wederom beperkt effect zal hebben. Waarom is er geen harde einddatum voor verplichte aansluiting op het Dezi-register voor de andere zorginstellingen? Is dit bewust gedaan en zo ja, waarom?

Het advies van de Afdeling advisering van de Raad van State om een harde einddatum op te nemen voor de verplichte overstap naar het Dezi-register is overgenomen. Deze einddatum wordt gesteld op 1 januari 2031 en komt terug in het wetsvoorstel.

De leden van de NSC-fractie zijn van mening dat de grootste verbetering in de digitale infrastructuur in de zorg teweeg kan worden gebracht als het nieuwe systeem maximaal benut wordt. Wat zou er volgens de regering nodig zijn om volledige deelname van alle systemen aan het Dezi-register te stimuleren?

Om dit te realiseren kiest de regering voor een gefaseerde wettelijke verplichtstelling die doorloopt tot 1 januari 2031. Daarnaast wordt brede deelname gestimuleerd door technische standaardisatie, certificering, ondersteuning bij implementatie en nauwe samenwerking met brancheorganisaties en leveranciers. Keuzevrijheid in inlogmiddelen en ruimte voor marktwerking gaan bijdragen aan lagere kosten en een betere aansluiting op het werkproces. Zo wordt het stelsel breed uitvoerbaar en betaalbaar, ook voor kleinere zorgaanbieders.

Voor zorgaanbieders specifiek is een stimuleringsregeling voorzien, waarbij in de eerste periode (2026/2027) wordt bijgedragen in de aanschaf van een nieuw inlogmiddel. Deze stimulering is bedoeld om zorginstellingen en haar medewerkers te bewegen over te stappen naar een veilig inlogmiddel binnen het nieuwe Dezi-stelsel. Vanaf het moment van de verplichtstelling kan de IGJ zo nodig handhavend optreden indien deelname door zorgaanbieders uitblijft.

De leden van de CDA-fractie lezen dat de regering voorstelt om alleen inlogmiddelen toe te staan die voldoen aan het betrouwbaarheidsniveau 'hoog'. Voor deze leden is niet helemaal duidelijk of deze keuze dwingend voortvloeit uit een wettelijke verplichting, of dat dit een beleidsmatige keuze betreft. Deze leden vragen hierop een reflectie.

De eIDAS-verordening schrijft niet voor dat voor het verwerken van medische gegevens betrouwbaarheidsniveau hoog is vereist. Uit de Algemene verordening gegevensbescherming (AVG) volgt wel dat persoonsgegevens door passende technische of organisatorische maatregelen op een dusdanige manier moeten worden verwerkt dat een passende beveiliging is gewaarborgd.[9] Volgens de Autoriteit Persoonsgegevens geldt voor medische persoonsgegevens betrouwbaarheidsniveau hoog.[10] Gezondheidsgegevens zijn namelijk per definitie gevoelig zodat een hoger beveiligingsniveau is vereist dan voor ander soorten persoonsgegevens. Wanneer sprake is van gegevens die onder het medisch beroepsgeheim vallen, dan wordt uitgegaan van een vereist betrouwbaarheidsniveau hoog, waardoor substantieel niet zou volstaan.

De leden van de CDA-fractie kunnen de keuze voor het betrouwbaarheidsniveau 'hoog' in principe volgen, maar vragen wel of de regering wil toelichten waarom het betrouwbaarheidsniveau 'substantieel' niet zou voldoen en wat daarin precies het verschil is met het niveau 'hoog'. Deze leden vragen waarom het bijvoorbeeld bij het inloggen bij MijnOverheid.nl wel toegestaan is (en voorlopig blijft) om in te loggen op het niveau 'substantieel'.

Het uitgangspunt van passende technische en organisatorische beveiligingsmaatregelen bepaalt het vereiste betrouwbaarheidsniveau.[11] Doordat gezondheidsgegevens per definitie gevoelig zijn, is een hoger beveiligingsniveau vereist dan voor andere type persoonsgegevens. Bij gegevens die vallen onder het medisch beroepsgeheim wordt uitgegaan van betrouwbaarheidsniveau hoog, zodat substantieel niet zou volstaan.[12] Het voorgaande is ook de reden waarom inloggen op MijnOverheid is toegestaan op betrouwbaarheidsniveau 'substantieel'. De opgevraagde gegevens in MijnOverheid vallen niet onder het medisch beroepsgeheim en eisen daardoor geen hoger betrouwbaarheidsniveau.

[9] Artikel 5, eerste lid, sub f en artikel 32 van de Algemene verordening gegevensbescherming.
[10] Brief Autoriteit Persoonsgegevens d.d. 28 november 2024, met kenmerk z2023-02938, blz. 4 en Kamerstukken II 2016-2017, 27 529, nr. 143, blz. 1.
[11] Artikel 5, eerste lid, sub f en artikel 32 van de Algemene verordening gegevensbescherming.
[12] Brief Autoriteit Persoonsgegevens d.d. 4 oktober 2018 met kenmerk z2018-17577 en Kamerstukken II 2016-2017, 27 529, nr. 143, blz. 1.

In Uitvoeringsverordening (EU) 2015/1502 staan de minimale technische specificaties, normen en procedures voor het voldoen aan betrouwbaarheidsniveau laag, substantieel en hoog.[13] Deze verordening werkt een onderdeel van de eIDAS-verordening verder uit.[14]

De Uitvoeringsverordening (EU) 2015/1502 werkt volgens een gelaagd systeem: om te voldoen aan betrouwbaarheidsniveau substantieel moet een elektronisch identificatiemiddel voldoen aan betrouwbaarheidsniveau laag én aan een van de opties uit de lijst van vereiste elementen voor betrouwbaarheidsniveau substantieel. Hetzelfde geldt voor het voldoen aan betrouwbaarheidsniveau hoog: minimaal voldoen aan betrouwbaarheidsniveau substantieel én aan een van de opties uit de lijst van vereiste elementen voor betrouwbaarheidsniveau hoog. Door dit systeem is betrouwbaarheidsniveau hoog veeleisender dan betrouwbaarheidsniveau substantieel.

Hieronder is een voorbeeld van hoe dit werkt met de vereiste elementen uit de Uitvoeringsverordening (EU) 2015/1502 voor het bewijzen en verifiëren van de identiteit van natuurlijke personen.[15]

Voor betrouwbaarheidsniveau substantieel kan gekozen worden voor optie 1. Hierin staan de volgende eisen: 1. Er is geverifieerd dat een persoon in bezit is van bewijs erkend door de lidstaat waar de aanvraag voor een elektronisch identificatiemiddel is gedaan en dat het bewijs de opgegeven identiteit vertegenwoordigt; 2. Dit bewijs is gecontroleerd op echtheid en; 3. Er zijn maatregelen genomen om het risico te minimaliseren dat de identiteit van de persoon niet overeenkomt met de opgegeven identiteit. Om vervolgens te voldoen aan betrouwbaarheidsniveau hoog, moet voldaan worden aan de bovenstaande eisen én aan bijvoorbeeld optie 1 voor betrouwbaarheidsniveau hoog. De vereiste elementen hiervan zijn: 1. Het controleren van een bewijs aan de hand van een gezaghebbende bron[16] en; 2 Het verifiëren van de opgegeven identiteit van een aanvrager door een vergelijking van een of meer fysieke kenmerken van de persoon met de gezaghebbende bron.

Voor betrouwbaarheidsniveau substantieel is dus de identiteitsverificatie minder strikt dan bij betrouwbaarheidsniveau hoog. Er zijn bijvoorbeeld geen eisen gesteld de fysieke kenmerken te controleren om een sterke koppeling tussen de natuurlijke persoon en het identificatiemiddel te borgen.

2.3 Identificatie en authenticatie voor toegang tot cliëntgegevens

De leden van de PVV-fractie vragen, voor welk platform is gekozen om de gegevensdeling van cliënten mogelijk te maken. Deze leden constateren dat er verschillende platformen beschikbaar zijn voor de gewenste inrichting, maar dat deze niet allemaal (volledig) met elkaar kunnen communiceren. Wat is hierover de visie van de regering?

Er zijn op dit moment inderdaad verschillende platformen en systemen voor gegevensuitwisseling. Deze zijn ontwikkeld met een eigen doel en zijn sectorspecifiek. Ik zie echter dat de markt de landelijke ontsluiting over systemen en sectoren heen niet op pakt. Daarom neem ik regie om bestaande systemen en infrastructuren te verbinden. Zo ontstaat een landelijk dekkend netwerk waarmee gezondheidsgegevens landelijk uitgewisseld kunnen worden.

Samen met het veld werk ik aan de realisatie van de Nationale visie en strategie (NVS) om databeschikbaarheid in 2035 voor het hele gezondheidsstelsel te realiseren. Om daarmee te zorgen dat gezondheidsgegevens altijd op de juiste plek en op het juiste moment en op een veilige wijze beschikbaar

[13] 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), overweging 2.

[14] 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 2014,* L257/73).

[15] 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).

[16] Artikel 1, onder 1 Uitvoeringsbesluit 2015//1502: een gezaghebbende bron is elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond.

zijn voor inwoner/cliënt en zorgverlener. Het verbinden van bestaande systemen en infrastructuren is een eerste stap richting het realiseren van de visie.

De leden van de GroenLinks-PvdA-fractie zijn nogmaals benieuwd naar de onderbouwing dat zorggegevens momenteel onvoldoende beschermd zijn. Op welke manier monitort de regering de oneigenlijke toegang tot zorggegevens? Hoe vaak komt dit voor dankzij de gebrekkige beveiliging van UZI-middelen?

De identificatie en autorisatie vindt in het huidige systeem plaats met de UZI-middelen. Deze UZI-middelen voldoen aan betrouwbaarheidsniveau hoog en zijn daarmee technisch goed beveiligd. Echter, vanwege het feit dat zorgaanbieders ook gebruik maken van andere inlogmiddelen met een lager betrouwbaarheidsniveau, maakt dat de zorggegevens desondanks niet voldoende zijn beschermd. Dit wordt met dit wetsvoorstel ondervangen door het voorschrijven van inlogmiddelen op het hoogste betrouwbaarheidsniveau. Ook is uit de praktijk gebleken dat de UZI-passen worden uitgeleend. Dit zal met de persoonlijke inlogmiddelen uit het Dezi-stelsel minder snel het geval worden.

Voor een geoorloofde toegang tot zorggegevens is niet alleen een geldige identificatie en authenticatie vereist, maar speelt ook autorisatie een grote rol. Wanneer de stappen van identificatie en authenticatie zijn doorlopen en duidelijk is dat de medewerker is wie hij stelt te zijn, dan heeft de betreffende medewerker nog de juiste rechten nodig om toegang te krijgen tot de zorggegevens waar het om gaat. Deze rechten worden door middel van een autorisatieproces door de zorgaanbieder aan de zorgmedewerker toegewezen.

Zorgaanbieders dienen de toegang tot zorggegevens te loggen. Wanneer blijkt dat oneigenlijke toegang heeft plaatsgevonden en dit een risico voor een betrokkene met zich heeft meegebracht, moet de zorgaanbieder dit als datalek melden bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens heeft geen aparte registratie van datalekken die zijn veroorzaakt door oneigenlijk gebruik van UZI-middelen. Het is daarom niet aan te geven hoe vaak dit voorkomt.

De leden van de GroenLinks-PvdA-fractie vragen om te onderbouwen waarom tot 1 januari 2029 nog het gebruik van UZI-middelen is toegestaan. Met de kennis dat deze middelen onveilig zijn, alternatieven voorhanden zijn, en het zorgveld al heeft kunnen experimenteren met DigiD als inlogmiddel, vragen deze leden waarom deze datum is verkozen in plaats van 1 januari 2027 of 1 januari 2028. Hoe verenigt de regering deze deadline met de grote urgentie om zorggegevens beter te beschermen?

De regering heeft gekozen voor een gefaseerde overgangsperiode tot uiterlijk 1 januari 2029 om zorgaanbieders voldoende tijd en ruimte te geven voor de overstap van het huidige UZI-stelsel naar het nieuwe Dezi-stelsel. Deze termijn is gebaseerd op de omvang en diversiteit van het zorgveld (van ziekenhuizen tot jeugdhulp en eerstelijnszorg), de noodzaak om softwareapplicaties en systemen aan te sluiten op het koppelvlak én de praktijkervaringen uit eerdere digitaliseringstrajecten waaruit blijkt dat een zorgvuldige, stapsgewijze implementatie een soepele overstap vergemakkelijkt.

De overgangsperiode is daarnaast gekozen om gebruikers van de huidige UZI-middelen enerzijds de geldigheidsduur van de middelen te laten benutten (een middel dat tot eind 2025 wordt uitgegeven heeft een geldigheid van drie jaar, dus tot eind 2028) en anderzijds de mogelijkheid te bieden tot een geleidelijke overgang naar een inlogmiddel dat binnen het Dezi-stelsel erkend is.

De leden van de GroenLinks-PvdA-fractie onderstrepen het belang van centrale regie om digitalisering in de zorg in goede banen te leiden. Zij volgen de analyse dat, zonder overheidsinterventie, de nodige ontwikkelingen niet van de grond komen. Echter vragen zij waarom de zorgsector deze ontwikkeling niet zelf zou toepassen, zonder interventie van de overheid. Waarom is de zorgsector er tot dusver niet in geslaagd om goede afspraken met elkaar te maken? Waarom wordt er nu pas ingegrepen om landelijke standaarden af te dwingen?

De afgelopen jaren heeft iedere zorgsector zich vooral gericht op de ontwikkeling van eigen EPD-systemen en de gegevensuitwisseling tussen EPD-systemen van dezelfde softwareleverancier. Hierdoor kunnen zorgaanbieders met het EPD-systeem van dezelfde softwareleverancier met elkaar gegevens uitwisselen. Maar het landelijk uitwisselen van gezondheidsgegevens tussen verschillende zorgaanbieders, sectoren en softwareleveranciers is onvoldoende door de markt opgepakt en dus nog steeds niet mogelijk.

Daarom neem ik meer regie om bestaande EPD-systemen en infrastructuren te laten verbinden. Zo ontstaat een landelijk dekkend netwerk waarmee gezondheidsgegevens landelijk en over sectoren heen

uitgewisseld kunnen worden. Die regie neem ik ook, omdat voorkomen moet worden dat databeschikbaarheid in de zorg een verdienmodel wordt en er spelers zijn die baat hebben bij een gefragmenteerd landschap. Toepassingen en diensten mogen wel concurreren op functionaliteiten die de bruikbaarheid van gegevens voor burgers en zorgverleners bevorderen. Zo blijft er ruimte voor innovatie.

De leden van de GroenLinks-PvdA-fractie vragen of de regering een soortgelijke noodzaak ziet in andere dossiers op het gebied van digitalisering in de zorg.

Naast regie op de realisatie van een landelijk dekkend netwerk van infrastructuren neem ik ook regie voor het realiseren van een landelijk vertrouwensstelsel en de generieke functies.

Landelijk vertrouwensstelsel

De laatste decennia zijn er verschillende afsprakenstelsels voor veilige gegevensuitwisseling ontwikkeld. Deze afsprakenstelsels ondersteunen één of meer sectoren of gegevenssets. In de afsprakenstelsels zijn onder andere afspraken vastgelegd die met vertrouwensaspecten te maken hebben, zoals over de manier van beveiliging van het communicatienetwerk of de te gebruiken standaarden voor identificatie. De vertrouwensmodellen van verschillende afsprakenstelsels komen in meer of mindere mate met elkaar overeen.

VWS heeft het Twiin Afsprakenstelsel gekozen als dé centrale plek voor de vastlegging van geharmoniseerde en gestandaardiseerde vertrouwensafspraken in de zorg. De keuze voor Twiin als landelijk vertrouwensstelsel heeft tot doel de versnippering van afspraken te verminderen door toe te werken naar meer uniformiteit en harmonisatie van bestaande oplossingen.

Generieke functies

Generieke functies bestaan uit sets van afspraken, standaarden en voorzieningen om de juiste gegevens op het juiste moment op de juiste plek te krijgen. Zoals lokalisatie, autorisatie en adressering. Vergelijk het met kentekenregistratie, rijbewijzen, verkeersborden en bewegwijzering. In eerdere brieven aan uw Kamer heb ik beschreven hoe ik regie heb genomen op generieke functies door inrichtingskeuzes te maken en deze met partijen in het zorgveld verder uit te werken. Voor de langere termijn onderzoek ik hoe (onderdelen van) de generieke functies verplicht gesteld kunnen worden.

De leden van de GroenLinks-PvdA-fractie vragen de regering om toe te lichten hoe zij de overstap naar Dezi-middelen gaat stimuleren, monitoren en evalueren.

Voor zorgaanbieders is een stimuleringsregeling voorzien. Deze stimulering is bedoeld om zorgverleners te bewegen over te stappen naar een veilig inlogmiddel binnen het nieuwe Dezi-stelsel. De overstap wordt gestimuleerd door bij te dragen in de aanschaf van een nieuw inlogmiddel voor de eerste twee jaar (2026/2027).

Ik onderken het belang van zorgvuldige monitoring en evaluatie bij de stapsgewijze overgang van het bestaande UZI-stelsel naar het nieuwe Dezi-stelsel. Tijdens de overgangsperiode (tot uiterlijk 1 januari 2029) worden zorgaanbieders gefaseerd aangesloten op het Dezi-register. Er worden indicatoren opgesteld om de voortgang te monitoren zodat tijdig kan worden bijgestuurd. Naast de indicatoren over het aantal aangesloten instellingen en zorgmedewerkers, wordt expliciet aandacht besteed aan de knelpunten zoals ervaren door zorgmedewerkers. De Kamer kan hierover desgewenst jaarlijks via een Kamerbrief over worden geïnformeerd.

Het CIBG zal periodieke voortgangsrapportages opleveren. Daarnaast wordt de IGJ structureel betrokken bij de evaluatie, zowel op het gebied van privacy, beveiliging als naleving van verplichtingen. Hun signalen worden meegenomen in de beleidsmatige doorontwikkeling van het stelsel. Ik houd ook de voortgang, de uitvoerbaarheid en de effecten van de overgang in het oog.

De leden van de GroenLinks-PvdA-fractie delen de zorgen rondom een 'vendor lock-in'. Zij vragen de regering toe te lichten wanneer er volgens haar sprake is van een gezonde concurrentie tussen leveranciers van inlogmiddelen. Hoe voorkomt de regering dat slechts één of enkele partijen naar boven drijven als hoofdleverancier?

Vendor-lock in wordt voorkomen door concurrentiemogelijkheden en keuzevrijheid te bieden tussen publieke, private, generieke én zorgspecifieke inlogmiddelen. Geen enkel zorginformatie- of gegevensuitwisselingssysteem mag één specifiek middel verplicht stellen. Dit wetsvoorstel voorziet in het

voorgestelde artikel 15 dat alle erkende middelen moeten kunnen worden gebruikt bij ieder systeem. Het CIBG faciliteert via een standaard koppelvlak toegang voor alle goedgekeurde inlogmiddelen.

De leden van de GroenLinks-PvdA-fractie vragen of de regering het net als deze leden een voorwaarde vindt dat er uitsluitend (of in ieder geval zo veel mogelijk) gebruik gemaakt wordt van Nederlandse en Europese inlogmiddelen, zodat de continuïteit in de zorg in geen enkel geval afhankelijk wordt van niet-Europese tech-leveranciers?

De continuïteit van zorg mag op geen enkel moment afhankelijk worden van een klein aantal of uitsluitend niet-Europese technologiebedrijven, zeker tegen de achtergrond van een veranderende geopolitieke context.

Het wetsvoorstel stelt in het voorgestelde artikel 15 dat zorgmedewerkers alle erkende inlogmiddelen moeten kunnen gebruiken bij de systemen van zorgaanbieders. Daarmee wordt voorkomen dat een middelenleverancier een blokkade opwerpt voor andere marktpartijen. De markt voor inlogmiddelen, ook die voor de zorgsector, is een volwassen en open markt met concurrentie. Ook nu al leveren marktpartijen toegangsmiddelen aan zorgaanbieders. Het wetsvoorstel geeft een grondslag om inlogmiddelen aan te bieden erkend door vier verschillende kaders: namelijk Wet digitale overheid, PKIoverheid, de eIDAS-verordening en NEN 7518. Hierdoor kunnen ICT-leveranciers via verschillende routes hun inlogmiddelen aanbieden.

De Dezi-inlogmiddelen worden erkend door de vier bovengenoemde kaders. Deze kaders stellen eisen en vragen om een officiële erkenning. Deze erkenning gebeurt door de Nederlandse overheid (op basis van de Wet digitale overheid en de PKIoverheid), op EU-niveau (bij de eIDAS-verordening), of door te voldoen aan de NEN-7518 (via een certificaat uitgegeven door een certificerende instelling onder de Raad van Accreditatie). Zowel de Wet digitale overheid als de NEN-7518 verwijzen naar de eIDAS-verordening. Dit alles 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.[17] Ook moeten verleners van vertrouwensdiensten onder toezicht staan van een nationale toezichthouder in een EU-land. Daarnaast moet de aanbieder voldoen aan alle technische en juridische eisen van eIDAS

Kortom, er zal uitsluitend gebruik gemaakt kunnen worden 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 GroenLinks-PvdA-fractie vragen hoe wordt afgedwongen dat de infrastructuur van het Dezi-register ook niet voor een deel afhankelijk wordt van de infrastructuur van niet-Europese tech-leveranciers. Erkent de regering het belang van strategische autonomie in de digitale zorg in de huidige geopolitieke context? Hoe waarborgt de regering dit binnen deze wetgeving?

Zoals aangegeven hierboven mag de continuïteit van onze zorg op geen enkele manier in het geding komen door de huidige geopolitieke verhoudingen en ontwikkelingen. Daarom levert het CIBG de infrastructuur van het Dezi-register, waardoor de infrastructuur onder mijn verantwoordelijkheid valt. Daarnaast is in het voorstel ruimschoots aandacht besteed aan het voorkomen van afhankelijkheid van (statelijke) actoren van buiten de Europese Unie wat betreft inlogmiddelen in de zorg. In dit kader is er daarom voor gekozen uitsluitend het gebruik van erkende inlogmiddelen toe te laten. Dit zijn middelen die vallen onder de Wet digitale overheid, PKIoverheid, de eIDAS-verordening, of die voldoen aan NEN 7518. Deze inlogmiddelen zijn erkend door de Nederlandse overheid, staan onder toezicht van de Europese Unie, of zijn gecertificeerd door een certificerende instelling onder de Raad van Accreditatie.

Daarmee zal dus de infrastructuur van het Dezi-register niet afhankelijk worden van niet- Europese tech-leveranciers, terwijl uitsluitend gebruikt gemaakt gaat worden van door Nederland erkende en/of onder

[17] Artikelen 2,14 en 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 (*PbEU 2014,* L257/73).

Europese toezicht staande inlogmiddelen. Hiermee wordt de continuïteit van de zorg in geen enkel geval volledig afhankelijk van niet-Europese tech-leveranciers.

De leden van de VVD-fractie zien dat in het wetsvoorstel regelmatig wordt verwezen naar de NEN-norm 7510. In 2023 liet de Inspectie Gezondheidszorg en Jeugd (IGJ) weten dat bijna alle ziekenhuizen voldoen aan deze norm maar een aantal nog niet. Voldoen inmiddels alle ziekenhuizen aan de norm?

Er zijn nog zes ziekenhuizen die er vooralsnog niet in zijn geslaagd om met een onafhankelijke toetsing aan te tonen dat zij voldoen aan de NEN-norm 7510 voor informatiebeveiliging. Een onafhankelijke beoordeling is echter wel een eis in de norm om aan te tonen dat aan de norm wordt voldaan.

Met elk van deze ziekenhuizen heeft de IGJ op regelmatige basis contact om de voortgang van lopende verbeteringen te monitoren. Meerdere van deze ziekenhuizen hebben op korte termijn een onafhankelijke toetsing gepland of moeten hiervoor binnenkort een herbeoordeling doen naar aanleiding van een eerdere toetsing.

De leden van de VVD-fractie vragen hoe de monitoring en evaluatie van de overstap wordt vormgegeven.

De regering onderkent het belang van zorgvuldige monitoring en evaluatie bij de stapsgewijze overgang van het bestaande UZI-stelsel naar het nieuwe Dezi-stelsel. Tijdens de overgangsperiode (tot uiterlijk 1 januari 2029) worden zorgaanbieders gefaseerd aangesloten op het Dezi-register. Monitoring vindt plaats op het aantal aangesloten organisaties en gebruikers per sector, het gebruik van erkende inlogmiddelen versus UZI-middelen, en de gemelde technisch, organisatorisch of juridisch knelpunten bij implementatie en gebruik.

Het CIBG zal periodieke voortgangsrapportages opleveren terwijl de IGJ tevens structureel wordt betrokken bij de evaluatie, zowel op het gebied van privacy, beveiliging als de naleving van verplichtingen. Hun signalen worden meegenomen in de beleidsmatige doorontwikkeling van het stelsel. Ik zal ook de voortgang, de uitvoerbaarheid en de effecten van de overgang in het oog houden.

De leden van de NSC-fractie noemen de samenwerking tussen digitale zorgsystemen (interoperabiliteit) als belangrijke voorwaarde om de administratieve lasten in de zorg terug te dringen. Deze leden vragen de regering in welke mate het Dezi-register interoperabel is met de andere zorgsystemen. Hoe kan dit in de toekomst worden verbeterd?

Interoperabiliteit kan worden bereikt door het gebruik van open standaarden. Dit zijn afspraken tussen ICT-systemen die door iedereen kunnen worden gebruikt. Alle (semi-) overheidsorganisaties hebben de verplichting open standaarden toe te passen die zijn opgenomen in de 'Pas toe of leg uit'-lijst van de Forum Standaardisatie [18], tenzij een zwaarwegende reden zich daartegen verzet.[19]

Het Dezi-stelsel is interoperabel omdat voor de technische koppelvlakken- die zorgen voor de uitwisseling van gegevens tussen informatiesystemen, een open standaard uit de genoemde lijst geldt.

Daarnaast wordt de interoperabiliteit van het Dezi-stelsel geborgd doordat de architectuur aansluit bij de algemene generieke architectuur van de eIDAS-verordening: de Architecture Reference Framework (ARF).[20] 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.

De verwachting is dat leveranciers deze architectuur zullen omarmen vanwege de rol bij bijvoorbeeld gegevensuitwisselingen op basis van de EHDS. De technische koppelvlakken waarmee Dezi werkt, zijn ook

[18] Deze lijst van open standaarden die geldt voor het Rijk, gemeenten en de provincies. Wanneer een ICT-dienst of product wordt aangeschaft en gebruikt maakt van de open standaard op de ‘pas toe leg uit’-lijst, dan moet van die standaard gebruik worden gemaakt (‘pas toe’). Uitzondering hierop is als er een zwaarwegende reden is om open standaard op de lijst af te wijken (‘leg uit’).

[19] Het Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. De leden worden op persoonlijke titel benoemd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

[20] eIDAS Expert Group, Architecture and reference framework, November 2023.

afgestemd met een aantal leveranciers van zorginformatiesystemen om te toetsen of zij de technische standaarden waar Dezi mee werkt daadwerkelijk in de praktijk kunnen toepassen.

Om de interoperabiliteit in het zorgveld met het oog op de toekomst verder te vergroten en daar sturing op te verrichten, wordt door VWS samen met het zorgveld gewerkt aan het landelijk dekkend netwerk van infrastructuren, generieke functies en aanpalende ICT-voorzieningen. Recent heb ik uw Kamer over de stand van zaken geïnformeerd.[21]

Hoewel er momenteel geen directe aanleiding is te komen tot een verbetering van de interoperabiliteit van het Dezi-register met andere zorgsystemen, borgt deze aanpak dat ook in de toekomst de standaarden die bijdragen aan het realiseren van interoperabiliteit met het veld worden afgestemd en vastgelegd.

De leden van de CDA-fractie steunen het voornemen van de regering, onder andere naar aanleiding van het advies van de Raad van State en de Autoriteit Persoonsgegevens (AP), om het gebruik van het Dezi-register en de bijbehorende middelen verplicht te stellen. Deze leden lezen dat de regering dit stapsgewijs wil doen en vragen wat dit precies betekent.

Het wetsvoorstel voorziet in een gefaseerde uitfasering van UZI-middelen tot uiterlijk 1 januari 2029. Gedurende deze overgangsperiode kunnen bestaande uitgegeven UZI-middelen nog worden gebruikt. Wanneer een zorgaanbieder of jeugdhulpverlener bij inwerkingtreding van dit wetsvoorstel nog niet klaar is om volledig over te stappen, biedt deze overgangstermijn ruimte voor stapsgewijze implementatie.

De leden van de CDA-fractie vragen of het klopt dat de overgangstermijn loopt tot 1 januari 2029 en zo ja, dan vragen zij waarom precies voor deze datum gekozen is. Genoemde leden vragen of de regering heeft overwogen deze datum naar voren te halen. Deze leden verwijzen naar het inloggen met DigiD bij MijnOverheid.nl, waarbij de keuze is gemaakt om het 'lage' betrouwbaarheidsniveau volledig uit te faseren per 1 juli 2028. Zij vragen waarom hier niet bij wordt aangesloten.

De regering heeft gekozen voor een gefaseerde overgangsperiode tot uiterlijk 1 januari 2029 om zorgaanbieders voldoende tijd en ruimte te geven voor de overstap van het huidige UZI-stelsel naar het nieuwe Dezi-stelsel. Deze termijn is gebaseerd op de omvang en diversiteit van het zorgveld (van ziekenhuizen tot jeugdhulp tot eerstelijnszorg) én de praktijkervaringen uit eerdere digitaliseringstrajecten waaruit blijkt dat een zorgvuldige, stapsgewijze implementatie een soepele overstap vergemakkelijkt.

Hoewel de noodzaak voor veilige en gebruiksvriendelijke gegevensuitwisseling groot is, is de vaart van de overstap afgestemd op de uitvoerbaarheid en beschikbaarheid van nieuwe en gecertificeerde inlogmiddelen. De overgangsperiode moet niet alleen technisch, maar ook organisatorisch haalbaar zijn, zonder extra werkdruk te leggen op zorgprofessionals. Daarom is een kortere overgangstermijn, zoals bijvoorbeeld wordt gehanteerd bij MijnOverheid.nl, onwenselijk.

Zorgaanbieders zijn verantwoordelijk voor de overstap, maar worden hierin ondersteund. Het CIBG en het Ministerie van VWS nemen een actieve regierol door, onder andere: het beschikbaar stellen van een standaard koppelvlak en technische documentatie, het begeleiden van leveranciers via pilots en implementatieondersteuning, het bieden van handreikingen, communicatie en een centrale servicedesk, en het faciliteren van kennisdeling tussen koplopers en andere organisaties. Daarnaast is voor zorgaanbieders in een stimuleringsregeling voorzien, waarbij in de eerste periode (2026/2027) wordt bijgedragen in de aanschaf van een nieuw inlogmiddel. Deze stimulering is bedoeld om zorginstellingen en haar medewerkers te bewegen over te stappen naar een veilig inlogmiddel binnen het nieuwe Dezi-stelsel.

Mocht blijken dat de overgang bij bepaalde sectoren of organisaties moeizaam verloopt, dan zullen VWS en het CIBG samen met betrokken partijen tijdig interventies inzetten. Dit kan bijvoorbeeld door gerichte ondersteuning op maat te realiseren, te bezien of inlogmiddelen versneld kunnen worden toegelaten of door andere praktische oplossingen voor tijdelijke overbrugging. Het doel blijft altijd om de werkdruk voor zorgaanbieders zoveel mogelijk te minimaliseren, terwijl tegelijkertijd de beweging naar een veiliger, toekomstbestendig toegangsmodel onverminderd doorgang vindt. De verplichte vervanging van alle andere inlogmiddelen met een lager betrouwbaarheidsniveau voor toegang tot elektronische zorginformatie- en gegevensuitwisselingssystemen heeft een overstaptermijn tot uiterlijk 1 januari 2031.

[21] Kamerstukken II 2024-2025, 27 529, nr. 331.

De leden van de SP-fractie constateren dat er met dit wetsvoorstel voor wordt gekozen om private ict-aanbieders een grotere rol te geven bij het aanbieden van toepassingen voor identificatie en authenticatie, hoewel er met DigiD ook nog een publieke optie blijft bestaan. Welke waarborgen zijn er ingebouwd om buitensporige winsten hiermee en vendor lock-ins te voorkomen? In hoeverre is de optie om een volledig publiek systeem te behouden onderzocht?

De erkende inlogmiddelen en elektronische zorginformatie- en gegevensuitwisselingssystemen worden gekoppeld aan een technisch platform dat door het CIBG wordt aangeboden. Hierdoor is er controle over de technische koppeling die gebruikt wordt door systemen voor zorginformatie en gegevensuitwisseling. Deze koppeling wordt technisch gerealiseerd via een open standaard. Dankzij deze open standaard, die door de overheid is vastgesteld, ontstaat een eenduidige werkwijze en stabiel koppelvlak dat niet door de leveranciers wordt bepaald. Dit voorkomt dat zorgaanbieders afhankelijk worden van één specifieke leverancier van inlogmiddelen (*vendor lock-in*) en bevordert de keuzevrijheid en samenwerking binnen de zorg. Doordat er verschillende inlogmiddelen beschikbaar kunnen komen in het Dezi-stelsel, met een terugvaloptie naar het publieke middel DigiD, geldt ook dat voor inlogmiddelen er geen gedwongen winkelnering hoeft te zijn en daarmee buitensporige winsten worden voorkomen. Met dit wetsvoorstel komt er uiteindelijk een verplichting om met de diverse goedgekeurde inlogmiddelen toegang te krijgen tot de SBV-Z, het Dezi-register en de zorginformatie- en gegevensuitwisselingssystemen. Om die reden kunnen zorgaanbieders dankzij dit wetsvoorstel niet in een vangnet van een *vendor-lock in* komen van een middelenleverancier.

Er is onderzocht of het een optie is dat het Ministerie van VWS zelf nieuwe inlogmiddelen gaat ontwikkelen om de huidige UZI-middelen te vervangen. Voor dit alternatief is niet gekozen omdat er al andere middelen op de markt zijn of worden ontwikkeld die gebruikt kunnen worden in de zorg. Hierbij kan gedacht worden aan DigiD, maar ook aan de zorgspecifieke inlogmiddelen die momenteel in ontwikkeling zijn. Aangezien er naar verwachting ook nog nieuwe zorgspecifieke inlogmiddelen bijkomen, is het niet nodig dat het Ministerie van VWS eigen middelen ontwikkelt.

2.4 Medewerkers registeren in het Dezi-register

De leden van de PVV-fractie merken op dat in artikel 14, lid 2 wordt gesteld 'Het Dezi-register wordt ingesteld en beheerd door Onze Minister'. Voorheen werd dit nog aangevuld met 'of een door Onze Minister aangewezen instelling.' Bij artikel 14a, lid 2, sub d wordt gerefereerd aan 'de inspectie'. Houdt dit hiermee verband? Kan dit worden toegelicht?

Artikel 14, tweede lid, van het wetsvoorstel sorteert voor op de keuze om het Dezi-register te beleggen bij het CIBG, dat als agentschap onder mijn verantwoordelijkheid valt. Artikel 14a, tweede lid, bevat een grondslag om nadere regels te stellen over het verstrekken van gegevens aan de IGJ of aan mij over het betrouwbaarheidsniveau van de inlogmiddelen.

De leden van de PVV-fractie merken op dat de artikelen 14 en 15 geheel worden herschreven. Wat eerder krachtens een algemene maatregel van bestuur werd geregeld, wordt nu keihard verankerd. Bijvoorbeeld artikel 15, lid 2 wordt artikel 14, lid 3, waarom is voor deze weg gekozen?

De huidige artikelen 14 en 15 van de Wabvpz zien specifiek op het UZI-register. Beide artikelen worden met dit wetsvoorstel alleen op noodzakelijke punten aangepast om zo het Dezi-systeem mogelijk te maken. Uit artikel 14, derde lid, van het wetsvoorstel volgt dat er vergoeding betaald moet worden voor inschrijving in het register. Dit stond eerst alleen in de algemene maatregel van bestuur. Het doel is deze grondslag verder te verduidelijken door het te verplaatsen naar dit wetsvoorstel. Daarnaast kon de mogelijkheid in artikel 15, tweede lid, van het wetsvoorstel, voorheen niet. Daarom kon dit daarvoor ook niet bij algemene maatregel van bestuur worden geregeld. Aangezien dit lid tevens een van de hoofdelementen is van dit wetsvoorstel, wordt dit nu geregeld bij wet.

De leden van de GroenLinks-PvdA-fractie hebben zorgen over de schaal van het Dezi-register. Eén centraal register, waarin Dezi-nummers, gekoppeld aan het BSN, van alle zorgmedewerkers geregistreerd staan, is mogelijk een aantrekkelijk doelwit voor cyberaanvallen. Welke gegevens van zorgpersoneel worden precies opgeslagen in het Dezi-register?

Bij de inschrijving van een zorgmedewerker worden de volgende gegevens in het register opgenomen: geslachtsnaam, geboortedatum, voornamen, adres, e-mailadres, burgerservicenummer, en, indien van toepassing, voor welke zorgaanbieder een zorgmedewerker werkzaam is, het BIG-nummer als bedoeld in artikel 1 van de Wet op de beroepen in de individuele gezondheidszorg, en de titel, als bedoeld in artikel 34 of artikel 36a van de Wet op de beroepen in de individuele gezondheidszorg.

De leden van de GroenLinks-PvdA-fractie vragen wie de 'sleutel' tot de persoonsgegevens in het Dezi-register in handen heeft.

Op grond van artikel 14, tweede lid, van het wetsvoorstel is de minister van VWS verantwoordelijk voor het stelsel ten aanzien van de identificatie en authenticatie van zorgverleners, inclusief het ontkoppelpunt. De minister is verantwoordelijk voor de verwerking van persoonsgegevens in het Dezi-register en het ontkoppelpunt. Het CIBG treedt op als uitvoeringsorganisatie van het ministerie van VWS.

De leden van de GroenLinks-PvdA-fractie vragen hoe het principe van dataminimalisatie wordt toegepast in de inrichting van het Dezi-register.

Dataminimalisatie wordt op verschillende wijzen toegepast. Bij het ontwerp en het implementatietraject is en wordt doorlopend beoordeeld welke gegevens noodzakelijk en proportioneel zijn in relatie tot het doel van de verwerking. Er worden alleen gegevens verwerkt die noodzakelijk zijn voor het uitvoeren van de taak, tenzij er voor de verwerking van die gegevens een andere grondslag bestaat. Ook wordt het archiveringsbeleid van het huidige register herijkt om vast te stellen of de bewaartermijnen van documenten die persoonsgegevens bevatten, niet langer zijn dan noodzakelijk.

De leden van de GroenLinks-PvdA-fractie vragen welke maatregelen de regering heeft genomen om de cyberveiligheid van deze gegevens te waarborgen.

Voor de informatiebeveiliging wordt het bestaande informatiebeveiligingsbeleid van het UZI-register voortgezet en daar waar nodig wordt het huidige informatiebeleid aangepast. Het CIBG voldoet bij de uitvoering van haar taken voor het UZI-register al aan diverse internationale en Europese standaarden, waaronder strenge informatiebeveiligingseisen. Een voorbeeld hiervan is een toepasselijke ETSI-standaard: de ETSI EN 319 401-*General Policy Requirements for Trust Service Providers*. Hierin worden onder meer eisen gesteld aan de logische en fysieke toegangsbeveiliging van de dienst. Het CIBG is hiervoor als vertrouwensdienst tevens gecertificeerd.

De leden van de GroenLinks-PvdA-fractie vragen of het Dezi-register wordt opgeslagen op Nederlands grondgebied en valt deze geheel onder het Nederlands recht? Zo nee, welke externen hebben (mogelijk) toegang tot het Dezi-register en heeft de regering de nodige veiligheidsanalyse (DPIA) en een exit-strategie opgesteld?

Het register wordt beheerd door het CIBG en wordt lokaal, binnen Nederlandse staatsgrenzen, versleuteld opgeslagen. Ook is Nederlands recht van toepassing. Met betrokken leveranciers zijn verwerkingsovereenkomsten afgesloten en vormen afspraken over de beëindiging van de dienst standaardonderdeel van de contractuele afspraken. Deze afspraken worden onder anderen vastgelegd in een *Business Continuity Plan*.

De leden van de GroenLinks-PvdA-fractie zijn benieuwd hoe medewerkers die geen Nederlandse identiteit hebben, en dus geen BSN, ook gebruik kunnen maken van het Dezi-register. Hoe kunnen zorgverleners zonder BSN veilig toegang verkrijgen tot zorggegevens? Zijn eIDAS-genotificeerde middelen hiervoor een oplossing?

Een Europese burger die een werkrelatie aangaat met een zorgaanbieder kan zich laten inschrijven als niet-ingezetene in de BRP (ook wel RNI, de Registratie van Niet-ingezetenen). Na inschrijving in de RNI krijgt deze persoon een BSN. De Europese zorgmedewerker kan zich registeren in het Dezi-register. Voor het verlenen van toegang kan gebruik gemaakt worden van een bestaande oplossing, namelijk de BRP-koppeling voor eIDAS.

De leden van de GroenLinks-PvdA-fractie vragen de regering om toe te lichten wat de status van stagiairs is binnen het nieuwe Dezi-register. Hoe worden stagiairs en zorgverleners-in-opleiding meegenomen in dit wetsvoorstel, zodat leertrajecten niet worden gehinderd door de nieuwe wetgeving?

Met dit wetsvoorstel kunnen beoogde medewerkers van zorg- en jeugdhulpaanbieders zich laagdrempelig inschrijven in het Dezi-register. Als er al een registratie in het UZI-register is ten aanzien van de stage- of opleidingsorganisatie, dan worden stagiairs en zorgverleners-in-opleiding automatisch gemigreerd naar het Dezi-register. Als er geen registratie in het UZI-register is, dan kunnen stagiairs en zorgverleners-in-opleiding voordat de stage of opleiding begint, zich inschrijven in het Dezi-register. Het wetsvoorstel hindert daarmee niet leertrajecten.

De leden van de VVD-fractie vragen wat de reden is dat een medewerker ingeschreven moet blijven staan als diegene niet meer werkzaam is in de zorg? In hoeverre zou het dan voor deze medewerker mogelijk zijn om toegang te krijgen tot cliënt- en patiëntgegevens?

Als een zorgmedewerker (tijdelijk) stopt met werken in de zorg, kan het toch zinvol zijn om ingeschreven te blijven staan in het Dezi-register. Door het behouden van de inschrijving in het Dezi-register kan de zorgmedewerker sneller en eenvoudiger terugkeren in de zorg. Het aanvragen van een nieuwe registratie kan namelijk de nodige tijd in beslag nemen. Een medewerker die niet meer werkzaam is in de zorg en ingeschreven staat in het Dezi-register, kan met alleen de registratie geen toegang krijgen tot cliënt- of patiëntgegevens. Een medewerker moet namelijk beschikken over een werkrelatie, een inlogmiddel en daarnaast via de zorgaanbieder toegang krijgen tot het systeem. De inschrijving van een zorgmedewerker in het Dezi-register is niet oneindig. Als een zorgmedewerker gedurende een periode van 7 jaar geen geregistreerde werkrelatie met een zorgaanbieder heeft gehad dan worden de gegevens verwijderd uit het register.

De leden van de CDA-fractie vragen hoe het uitschrijven uit het nieuwe Dezi-register zal plaatsvinden als iemand niet meer in de zorg werkt. Deze leden vragen wie daarvoor verantwoordelijk is, de medewerker of de zorgaanbieder, en hoe dat precies in de praktijk verloopt.

Zodra een zorgmedewerker niet meer binnen de zorg werkzaam is, kan die een verzoek indienen voor doorhaling in het Dezi-register. De verantwoordelijkheid hiertoe ligt bij de zorgmedewerker. Wanneer de werkrelatie tussen zorgmedewerker en zorgaanbieder wordt verbroken, is het de verantwoordelijkheid van de zorgaanbieder om deze mutatie direct in het register door te voeren. Hiermee wordt de registratie van een zorgmedewerker veranderd; de koppeling met de zorgaanbieder wordt verwijderd uit de registratie van de zorgmedewerker. Een zorgmedewerker kan dan ook geen gebruik meer maken van eerder verkregen autorisaties en heeft dus geen toegang tot de systemen van de zorgaanbieder.

De inschrijving van een zorgmedewerker is bovendien niet oneindig. Als een zorgmedewerker gedurende een periode van 7 jaar geen geregistreerde werkrelatie met een zorgaanbieder heeft gehad, worden diens gegevens verwijderd uit het register.

2.5 Inlogmiddelen met het betrouwbaarheidsniveau hoog

De leden van de PVV-fractie vragen of in de wijzigingsopdracht voor artikel 14a, sub d, met 'inspectie' de IGJ wordt bedoeld.

Met "inspectie' wordt inderdaad de IGJ bedoeld. Dit is gedefinieerd in artikel I, onderdeel A, van de Verzamelwet gegevenswerking VWS II.a, die de Wapvpz gaat wijzigen.[22]

De leden van de GroenLinks-PvdA-fractie pleiten voor een zorgvuldig proces om vast te stellen dat nieuwe inlogmiddelen voldoen aan de gestelde eisen. Zij vragen om een uitleg hoe het goedkeuringsproces er precies uitziet en hoe het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) de benodigde bewijsmiddelen zal controleren.

De goedkeuringsprocedures voor de inlogmiddelen in het Dezi-stelsel wordt de komende tijd nader vormgegeven. Deze algemene maatregel van bestuur wordt voorgehangen. Er kan voor nu wel een algemene uitleg worden gegeven over hoe het goedkeuringsproces eruit gaat zien.

<u>Wet Digitale Overheid</u>
Inlogmiddelen in de zin van de Wet digitale overheid worden van rechtswege goedgekeurd wanneer zij voldoen aan betrouwbaarheidsniveau hoog.

[22] Artikel I, onderdeel A, Verzamelwet gegevensverwerking VWS II.a (*Stb. 2025, 83).*

eIDAS-verordening
Een inlogmiddel op basis van de eIDAS-verordening wordt goedgekeurd wanneer het inlogmiddel door een lidstaat is aangemeld bij de Europese Commissie en het voldoet aan de eisen van betrouwbaarheidsniveau hoog.

PKI-o-servicecertificaten
Een PKI-o-servicecertificaat wordt op aanvraag goedgekeurd wanneer het is uitgegeven door een vertrouwensdienst in de zin van de eIDAS-verordening, het voldoet aan een betrouwbaarheidsniveau gelijkwaardig aan *Organization Validated* én een uniek identificerend kenmerk heeft.[23] Dit kenmerk kan worden verkregen via het CIBG.

Zorgspecifieke inlogmiddelen
Voor zorgspecifieke inlogmiddelen moet een conformiteitscertificaat (verkregen na een audit) aan het CIBG worden overlegd. Hieruit moet volgen dat zowel het inlogmiddel als de verstrekkende partij voldoen aan de gestelde eisen. Het CIBG controleert of het conformiteitscertificaat is uitgegeven door een conformiteitsbeoordelingsinstantie (CI) die gerechtigd is om een audit op de toepasselijke norm (NEN 7518) uit te voeren en of deze audit op de juiste elementen heeft plaatsgevonden. De CI kan alleen een audit uitvoeren als zij hiertoe zijn aangewezen door de Raad van Accreditatie. Tevens zal er een controle plaatsvinden of de leverancier van een inlogmiddel is opgenomen in het Europese vertrouwenslijst van partijen die inlogmiddelen op betrouwbaarheidsniveau hoog uitgeven.

De leden van de GroenLinks-PvdA-fractie vragen de regering of zij kan toezeggen dat zij goedkeuringen van nieuwe middelen zo transparant mogelijk aan de Kamer zal doen toekomen en te publiceren, zodat de documentatie over deze middelen vindbaar en verifieerbaar is?

Het voornemen is om een overzicht te publiceren van inlogmiddelen die zijn goedgekeurd.

De leden van de NSC-fractie zijn erg voorzichtig met het gebruik van algoritmes op gevoelige persoonsgegevens. Mag de data in het Dezi-register ook voor andere doeleinden worden gebruikt? Zo ja, voor welke doeleinden en welke algoritmes worden op deze data toegepast?

Het gebruik van data in het Dezi-register mag alleen voor de doelen omschreven in dit wetsvoorstel. Deze doelen zijn het beheer van het register en de goedkeuring van inlogmiddelen.

De leden van de CDA-fractie lezen dat de regering kiest voor het uitgangspunt van keuzevrijheid voor inlogmiddelen. Deze leden vragen of deze keuze zich wel verhoudt tot de doelstelling om te komen tot meer standaardisatie en het terugdringen van fragmentatie. Deze leden vragen of de regering hierop wil reageren.

De regering onderkent het spanningsveld tussen keuzevrijheid en standaardisatie en deelt het uitgangspunt dat fragmentatie moet worden teruggedrongen. Tegelijkertijd is het uitgangspunt van keuzevrijheid voor inlogmiddelen bewust gekozen binnen het Dezi-stelsel. Keuzevrijheid draagt bij aan toegankelijkheid en innovatie en sluit daarnaast aan bij de diverse werkpraktijken in de zorg. De keuzevrijheid geldt uitsluitend binnen een duidelijk afgebakend kader: alle inlogmiddelen moeten voldoen aan het betrouwbaarheidsniveau hoog. Daarnaast is aansluiting op het standaard koppelvlak verplicht. Hierdoor ontstaat een situatie waarin alle middelen interoperabel zijn, ongeacht de leverancier. Fragmentatie in termen van techniek en beveiligingsniveaus wordt hiermee voorkomen.

De leden van de CDA-fractie vragen of het niet veel wenselijker is dat zoveel mogelijk zorgaanbieders en zorgverleners gebruik maken van één (of slechts enkele) inlogmiddel(en), vanuit het oogpunt van eenvoud, overzicht en het verminderen van fragmentatie.

De zorg is een complexe sector met uiteenlopende werkcontexten: van ziekenhuiszorg tot wijkverpleging, en van jeugdhulp tot GGZ. Eén enkel inlogmiddel past zelden overal goed bij. Juist keuzevrijheid maakt het

[23] Een PKI-o-servicecertificaat is een erkend servicecertificaat uitgegeven aan apparaten, (computer)servers of groepen personen op basis van het PKI-O afsprakenstelsel. Voor het verlenen van een certificaat met betrouwbaarheidsniveau 'Organization Validated' verifieert de vertrouwensdienst eerst de identiteit en locatie van de organisatie in kwestie.

mogelijk een inlogmiddel te kiezen dat aansluit bij de werkpraktijk, zoals: een fysieke pas, een smartphone-app, of een integratie met bestaande ziekenhuispas.
Het voorschrijven van één middel zou de uitvoerbaarheid, acceptatie en gebruiksvriendelijkheid in gevaar brengen. Tegelijkertijd wordt met de verplichte aansluiting op het koppelvlak geborgd dat (al) deze inlogmiddelen ten minste interoperabel zijn.

De leden van de CDA-fractie zijn ook van mening dat zo'n keuze administratieve lasten kan verminderen, omdat minder inlogmiddelen hoeven worden gecertificeerd en geaccrediteerd. Deze leden vragen of de regering deze mening deelt.

Hoewel keuzevrijheid meerdere aanbieders impliceert, wordt de certificering daarvan gebundeld via een gestandaardiseerd toetsingskader, namelijk de NEN 7518 en een gecentraliseerd toezicht. De grootste lasten van certificering ligt niet bij zorgmedewerkers of zorgaanbieders, maar bij de aanbieders van de inlogmiddelen. Tegelijkertijd worden zorgorganisaties juist ontlast doordat zij geen aparte inlogsystemen meer hoeven te onderhouden: elk erkend middel werkt via dezelfde standaard.

De leden van de CDA-fractie vragen waarom de regering er niet voor kiest om inloggen via het systeem van DigiD en/of eHerkenning als uitgangspunt te nemen, eventueel een aangepaste versie hiervan specifiek voor de zorg, indien nodig aangevuld met enkele zorgspecifieke inlogmiddelen. De leden vragen of de regeling hiervan de voor- en nadelen wil schetsen en de haalbaarheid hiervan wil verkennen en of dit leidt tot lagere kosten. Zij vragen voorts of de regering hierbij specifiek wil ingaan op het systeem van eHerkenning, waarbij de rijksoverheid samenwerkt met enkele erkende leveranciers. Deze leden vragen in hoeverre dit systeem verschilt van het voorgestelde systeem in dit wetsvoorstel en in hoeverre zo'n systematiek ook in de zorg gebruikt kan worden.

Er is onderzocht of hergebruik van de onderliggende techniek van DigiD of het eHerkenningsstelsel mogelijk en wenselijk zou kunnen zijn. Echter, deze systemen bleken qua architectuur en technische standaarden onvoldoende passend. Beide hanteren namelijk een minder moderne technische standaard en zijn mede doordoor complex in het realiseren van een aansluiting door een zorgaanbieder. Dat is onwenselijk binnen het gefragmenteerde zorglandschap met aanzienlijk meer zorgaanbieders dan momenteel zijn aangesloten bij DigiD en eHerkenning.

Om die reden is bij het ontwerp van Dezi goed gekeken naar de opzet en de sterke en zwakke punten van de DigiD, eHerkenning en van grote toegangsoplossingen zoals de ToegangsVerleningService (TVS)[24] van het ministerie van BZK, SURFconext[25] (ten behoeve van het hoger onderwijs) en de infrastructuur voor inloggen die door VWS is gerealiseerd tijdens de Coronapandemie.

Daarbij is het van belang te benadrukken dat de daadwerkelijke authenticatie-laag slechts een onderdeel vormt van de totale oplossingsarchitectuur. De kern van het systeem wordt gevormd door een registerstructuur waartoe zorgverleners zich op een hoog betrouwbaarheidsniveau dienen te authentiseren voor het verkrijgen van een zorgidentiteit.

Hoewel het fundamenteel herinrichten van DigiD of het eHerkenningsstelsel als technisch en organisatorisch complex is beoordeeld, is gekozen om wél aansluiting te zoeken bij de door deze stelsels erkende inlogmiddelen voor gebruik door de zorgprofessional. Op dat punt fungeren DigiD en eHerkenning dus als uitgangspunt. Het hergebruik van de erkende inlogmiddelen, zoals DigD, is beoogd om de administratieve lasten te beperken. Voor de identificatie en authenticatie van natuurlijke personen – de zorgmedewerkers – wordt aangesloten bij het wettelijk kader van de Wet digitale overheid, waaronder ook DigiD en eHerkenning vallen. Dit impliceert dat erkende Wdo-middelen die een BSN kunnen leveren, rechtstreeks toepasbaar zijn als Dezi-inlogmiddel.

Daarnaast bestaat binnen het zorgveld een substantiële behoefte aan aanvullende, zorgspecifieke authenticatiemiddelen. De Wdo voorziet echter niet in de erkenning van dergelijke zorgspecifieke middelen. De Wdo-erkende middelen moeten universeel beschikbaar zijn voor alle burgers en toepasbaar zijn bij publieke dienstverlening, zoals MijnOverheid of de Belastingdienst. Zorgspecifieke middelen daarentegen worden uitgegeven onder verantwoordelijkheid van individuele zorgaanbieders en zijn enkel

[24] De ToegangsVerleningService is een dienst die het mogelijk maakt om de digitale dienstverlening van een organisatie via inlogmiddelen zoals eHerkenning en DigiD toegankelijk te maken voor ondernemers en burgers.
[25] SURFconext is een dienst van SURF die het mogelijk maakt dat studenten in het MBO en HO via inlogmiddelen van de onderwijsinstelling waarbij zij zijn ingeschreven ook onderwijs en diensten bij derden kunnen afnemen.

toegankelijk voor zorgmedewerkers met een formele werkrelatie tot deze instellingen. Bovendien ontsluiten zorgspecifieke middelen géén BSN, maar een afgebakende zorgidentiteit. In de zorgidentiteit staat een Dezi-nummer, naam en zorginstelling. Om zorgspecifieke middelen te kunnen erkennen, is dus een afzonderlijk toetsingskader vereist buiten de reikwijdte van de Wdo.

Een laatste reden is gelegen op het gebied van de verstrekking van gekwalificeerde attributen, waardoor het register kan fungeren als Europese vertrouwensdienst, als bedoeld in de eIDAS-verordening. Het huidige UZI-stelsel kent in functionele zin namelijk twee hoofdcomponenten: enerzijds een register, en anderzijds voorzieningen voor de identificatie en authenticatie van natuurlijke personen (zorgprofessionals) en organisaties (inclusief hun ICT-systemen). Concreet betreft dit het UZI-register, de UZI-pas en UZI-servercertificaten.

In de toekomstige inrichting van het stelsel worden deze componenten vervangen of gemigreerd naar alternatieve oplossingen. Een wezenlijk element binnen deze transitie is de vervanging van het UZI-register door het Dezi-register. Deze migratie omvat niet alleen de verandering van het register zelf, maar ook alle bijbehorende processen en koppelingen met bronregisters zoals: de BRP, het BIG-register en het Diplomaregister. De nieuwe oplossing is afgestemd op de Europese referentiearchitectuur (ARF), met als doel het Dezi-register in te richten als een register dat gekwalificeerde attributen kan verstrekken ('Qualified Electronic Attestation of Attributes').[26] DigiD noch het eHerkenningsstelsel kunnen deze rol vervullen, dit zijn immers geen registers. Het voeren van het Dezi-register is een in de wet benoemde taak waardoor het register ook kan fungeren als erkende Europese vertrouwensdienst, zoals de eIDAS-verordening dat voorschrijft.

De leden van de CDA-fractie begrijpen dat er praktijksituaties zijn die andere vormen van inlogmiddelen vereisen dan DigiD en/of eHerkenning (zoals in de OK of bij een MRI-scanner), maar vragen of de regering kan schetsen hoe vaak dit voorkomt. Deze leden vragen of niet in het overgrote deel van de gevallen gebruik gemaakt wordt of kan worden van computer/PC, tablet of smartphone, en daarmee dus ook van één of enkele digitale inlogmiddelen zoals DigiD.

In de zorg is de toegang tot zorginformatie- en gegevensuitwisselingssystemen net als op veel werksituaties geregeld via een combinatie van werkstations, tablets en smartphones. In bepaalde gevallen moet ook met specifieke medische apparatuur worden gewerkt. Hierbij is niet alleen de veiligheid en hygiëne van belang, maar ook de snelheid en gebruiksvriendelijkheid van de gebruikte inlogmethoden. De keuze voor het juiste inlogmiddel hangt daarbij sterk af van de werksituatie van de zorgverlener. In een vaste werkomgeving, bijvoorbeeld een balie of spreekkamer, kan een inlogmiddel zoals DigiD goed werken. Echter, in een meer dynamische werksituaties, zoals de thuiszorg, de OK of op de Spoedeisende Hulp, is het belangrijk dat het inlogmiddel snel en eenvoudig te gebruiken is, zodat zorgverleners geen tijd verliezen bij het toegang krijgen tot belangrijke informatie. Hierop aansluitend worden de toegangsmiddelen vaak gecombineerd met andere functies, zoals bijvoorbeeld het openen van deuren (fysieke toegang tot bepaalde ruimtes) of een laagdrempelige identificatie van de zorgmedewerker aan de patiënt/cliënt door een foto en een naam op een fysieke toegangspas.

Wanneer er slechts één of enkele digitale inlogmiddelen zoals DigiD beschikbaar zouden zijn, dan zouden de bovengenoemde functionaliteiten ook moeten worden geharmoniseerd over alle zorgaanbieders. Dat ligt niet voor de hand.

Dit wetsvoorstel biedt ruimte voor verschillende soorten inlogmiddelen, zodat zorgaanbieders en zorgverleners zelf kunnen kiezen welk middel het beste aansluit bij hun specifieke werk- en gebruikssituatie en functionele behoeften. Het voorschrijven van slechts één of enkele inlogmiddelen, zoals DigiD, is niet geschikt voor alle zorgprocessen en alle behoeften en kan veel weerstand oproepen, zo blijkt uit ervaringen met de UZI-pas.

De leden van de CDA-fractie lezen dat de regering beargumenteert dat via keuzevrijheid een «vendor lock-in» kan worden voorkomen, in die zin dat zorgaanbieders niet afhankelijk zijn van één leverancier. Deze leden delen het belang van back-ups, maar zien juist ook voordelen van een uniforme aanpak, net als die we bij DigiD kennen,

[26] Een Qualified Electronic Attestation of Attributes is een officieel digitaal bewijs van een bepaald kenmerk van een persoon of organisatie. Voorbeelden hiervan zijn diploma's of een beroepsregistratie. Een QEAA wordt uitgegeven door een erkende partij en is juridisch gelijkwaardig aan een papieren bewijs.

omdat daar het probleem van «vendor lock-in» ook niet speelt. Deze leden vragen of dit klopt en of de regering op dit argument wil ingaan.

Het wetsvoorstel zorgt juist voor een uniforme aanpak. Dit gebeurt op drie manieren. Ten eerste, door het gebruik van goedgekeurde inlogmiddelen. Ten tweede, door aanbieders van voorzieningen zoals de SBV-Z en het Dezi-register te verplichten het gebruik van goedgekeurde inlogmiddelen mogelijk te maken. Ten derde, door gebruik van andere elektronische uitwisselingssystemen en zorginformatiesystemen mogelijk te maken met deze goedgekeurde inlogmiddelen. De goedgekeurde inlogmiddelen worden gekoppeld aan een technisch platform dat door het CIBG wordt aangeboden. Hierdoor is er controle over de technische koppeling die gebruikt wordt door systemen voor zorginformatie en gegevensuitwisseling. Deze koppeling wordt technisch gerealiseerd via een open standaard. Dankzij deze open standaard, die door de overheid is vastgesteld, ontstaat een eenduidige werkwijze en een stabiel koppelvlak dat niet door de leveranciers wordt bepaald. De uniforme aanpak en het toepassen van de standaarden voorkomt dat zorgaanbieders afhankelijk worden van één specifieke leverancier (*vendor lock-in*) en bevordert daarnaast de keuzevrijheid en samenwerking binnen de zorg. Doordat er verschillende goedgekeurde inlogmiddelen beschikbaar kunnen komen in het Dezi-stelsel, met een terugvaloptie naar het publieke middel DigiD, geldt ook dat voor inlogmiddelen er geen gedwongen winkelnering hoeft te zijn.

De leden van de CDA-fractie benadrukken het belang van het verminderen van afhankelijkheden van (statelijke) actoren van buiten de Europese Unie. Deze leden vragen of de regering deelt dat het niet veel verstandiger is om alleen gebruik te maken van bestaande door de overheid ontwikkelde inlogmiddelen zoals DigiD of mogelijke nieuwe inlogmiddelen die worden ontwikkeld door of binnen de EU.

De continuïteit van zorg mag op geen enkel moment afhankelijk worden van een klein aantal of uitsluitend niet-Europese technologiebedrijven, zeker tegen de achtergrond van een veranderende geopolitieke context.

De Dezi-inlogmiddelen in dit wetsvoorstel worden erkend op grond van vaste kaders: de Wet digitale overheid, PKI-overheidsstelsel, de eIDAS-verordening en de NEN 7518. Elk van deze kaders stelt eisen en vraagt om een officiële erkenning. Deze erkenning gebeurt door de Nederlandse overheid (Wet digitale overheid en PKI-overheidsstelsel), op EU-niveau (eIDAS-verordening) of door te voldoen aan de NEN 7518 (middels een certificaat uitgegeven door een certificerende instelling onder Raad van Accreditatie). Zowel de Wet digitale overheid als de NEN 7518 verwijzen naar de eIDAS-verordening.

Dit betekent dat alleen inlogmiddelen kunnen worden gebruikt die zijn erkend door de Nederlandse overheid of die onder toezicht staan van de Europese Unie. Daarnaast schrijft de eIDAS-verordening voor dat een verlener van een vertrouwensdienst 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.[27] Ook moet een verlener van vertrouwensdiensten onder toezicht staan van een nationale toezichthouder in een EU-lidstaat. Daarnaast moet de aanbieder voldoen aan alle technische en juridische eisen van eIDAS.

Daarmee zal uitsluitend gebruik gemaakt kunnen worden van door Nederland erkende en/of onder Europese 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 CDA-fractie vragen of het via dit wetsvoorstel, al dan niet bij of krachtens algemene maatregel van bestuur, mogelijk is om nadere eisen te stellen aan inlogmiddelen met het oog op de nationale veiligheid en de strategische autonomie.

De mogelijkheden om nadere eisen te stellen aan inlogmiddelen met het oog op de nationale veiligheid en strategische autonomie liggen niet in deze wet. In dat geval zullen deze eisen, indien nodig, opgenomen moeten worden in de Wet digitale overheid, de eIDAS-verordening, of de NEN 7518, die de basisvereisten vormen voor de toegelaten middelen.

[27] Artikelen 2,14 en 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 (PbEU 2014, L257/73).

De leden van de CDA-fractie vragen of het mogelijk is om bijvoorbeeld via algemene maatregel van bestuur een maximumaantal inlogmiddelen vast te leggen.

Binnen het huidige wetsvoorstel zijn er geen mogelijkheden om een maximumaantal inlogmiddelen vast te leggen. Dit past, naar idee van de regering, ook niet binnen de principes van een open markt.

2.5.1 Wdo erkende inlogmiddelen

De leden van de GroenLinks-PvdA-fractie vragen of de regering het ontwikkelen van Wdo erkende inlogmiddelen wil stimuleren, en zo ja, hoe en of dit ook geldt voor inlogmiddelen die breder inzetbaar zijn dan alleen de zorg.

De regering ziet het gebruik van Wdo-erkende inlogmiddelen als één van de mogelijke routes om veilige digitale toegang in de zorg te realiseren, mits deze inlogmiddelen voldoen aan het vereiste betrouwbaarheidsniveau hoog en goed aansluiten bij zorgprocessen. De regering kiest nadrukkelijk voor een open stelsel waarin zowel Wdo-erkende als zorgspecifieke inlogmiddelen worden toegelaten, mits deze laatstgenoemde zijn gecertificeerd conform de geldende normen, zoals NEN 7518. Er is op dit moment geen gerichte stimulering vanuit VWS richting het ontwikkelen van Wdo-middelen, noch voor inlogmiddelen die breder inzetbaar zijn dan alleen de zorg.

De leden van de GroenLinks-PvdA-fractie vragen of het Ministerie van Volksgezondheid, Welzijn en Sport samenwerkt met de Ministeries van Economische Zaken en Binnenlandse Zaken om te komen tot betrouwbare Nederlands-Europese alternatieve inlogmiddelen.

Er is geen specifieke samenwerking met andere ministeries gericht op het creëren van Nederlandse of Europese inlogmiddelen via de Wet digitale overheid. Wel vindt er beleidsafstemming met BZK plaats over de interoperabiliteit van publieke inlogmiddelen, zoals DigiD en de Europese wallet, in het kader van toegang.

De leden van de GroenLinks-PvdA-fractie vragen of de regering een praktisch beeld kan schetsen van hoe zorgmedewerkers Wdo-erkende inlogmiddelen gebruiken in hun dagelijkse werk en wat patiënten hiervan merken.

Voor zorgmedewerkers betekent dit dat zij, afhankelijk van hun zorginstelling, gebruik kunnen maken van erkende inlogmiddelen die aansluiten bij hun werkpraktijk. Dit kan bijvoorbeeld (in de toekomst) door gebruik van de wallet te maken bij het inloggen. Deze wallet maakt het inloggen in bijvoorbeeld de thuiszorg ook mogelijk. Patiënten merken hier in de praktijk niets van: zij zien geen verandering in hoe zij zorg ontvangen, maar mogen er wél op vertrouwen dat hun gegevens beter beschermd zijn door de inzet van veilige en gecertificeerde toegangsmiddelen.

2.5.2 Zorgspecifieke inlogmiddelen (gecertificeerd op basis van de NEN 7518)

De leden van de GroenLinks-PvdA-fractie willen weten welk aandeel van de (jeugd)zorgsector momenteel gebruik maakt van zorgspecifieke inlogmiddelen.

Ik heb thans geen zicht op het huidige gebruik van zorgspecifieke middelen door zorgaanbieders. Echter, vanuit de diversiteit aan zorg en jeugdhulp in Nederland begrijp ik hun behoefte om een middel te (blijven) gebruiken dat specifiek passend is op het betreffende zorgproces.

De leden van de GroenLinks-PvdA-fractie vragen hoe wordt toegezien dat, los van het certificeren, bestaande zorgspecifieke inlogmiddelen wel met spoed aan de nieuwe wettelijke standaarden voldoen. Is dit een taak van de Minister van VWS, de NEN-werkgroep, de Raad voor Accreditatie, certificerende instellingen of zorgaanbieders zelf?

Binnen het Dezi-stelsel kunnen alleen zorgspecifieke middelen gebruikt worden die voldoen aan de eisen van de NEN 7518 en daarmee ook aan betrouwbaarheidsniveau hoog. Het is de verantwoordelijkheid van de zorgaanbieder om aan de hand van een conformiteitscertificaat, die verkregen wordt na een audit door een conformiteitsbeoordelingsinstantie, bij het CIBG aantoonbaar te maken dat het gebruikte zorgspecifieke middel voldoet. Voldoet het niet, dan wordt het zorgspecifieke middel niet goedgekeurd en kan het middel niet worden gebruikt in het Dezi-stelsel.

De leden van de NSC-fractie willen de regering vragen hoe het wetsvoorstel zich verhoudt tot de NEN 7518 en NEN 7510-normen.

De NEN 7518 is de norm waarmee zorgaanbieders gecertificeerd kunnen worden om, onder hun eigen verantwoordelijkheid, een zorgspecifiek inlogmiddel beschikbaar te stellen aan hun medewerkers. Deze inlogmiddelen worden erkend op basis van een certificaat dat is afgegeven door een certificerende instelling die onder toezicht staat van de Raad voor Accreditatie. Het wetsvoorstel verwijst naar de NEN 7518 als officieel kader voor deze certificering.

De NEN 7510 gaat over informatiebeveiliging in de zorg, zoals het beschermen van medische gegevens. De NEN 7510 is niet het normenkader waarmee zorgaanbieders hun inlogmiddelen kunnen laten certificeren. Daarvoor geldt NEN 7518.

De leden van de SP-fractie lezen dat zorgaanbieders voor het uitgifte-proces van inlogmiddelen ook gecertificeerd moeten worden. Kan de regering een inschatting maken van de regeldrukeffecten die dit met zich mee zal brengen?

Het is lastig een inschatting te maken van de regeldrukeffecten. Er is hier namelijk geen sprake van een verplichting, zodat onzeker is of en hoeveel zorgaanbieders gebruik zullen maken van deze mogelijkheid. Zorgaanbieders hebben, naast een NEN-gecertificeerd inlogmiddel, namelijk ook de keuze voor inlogmiddelen die al op basis van de Wdo of eIDAS-verordening zijn goedgekeurd.

De inschatting van betrokken experts is dat op basis van het certificeringsschema (NCS7518) bij de NEN 7518 het uitvoeren van de audit om te komen tot een certificaat van conformiteit met de NEN 7518 één tot twee dagen vraagt.

2.5.3 PKI-o-certificaten

Geen opmerkingen of vragen van de fracties.

2.5.4 Onder de eIDAS-verordening genotificeerde inlogmiddelen

De leden van de GroenLinks-PvdA-fractie horen graag op welke termijn naar verwachting de eIDAS-genotificeerde inlogmiddelen beschikbaar zullen zijn en wanneer deze in de zorg ingezet kunnen worden.

De eerste eIDAS-genotificeerde elektronische identificatiemiddelen zijn sinds 29 september 2018 beschikbaar. Sinds die datum is de grensoverschrijdende erkenning van deze middelen binnen de EU van kracht, zoals vastgelegd in de eIDAS-verordening. Sindsdien hebben meerdere EU-lidstaten hun nationale eID-schema's genotificeerd.

De notificatie van eHerkenning onder de eIDAS-verordening was op 13 september 2019 en de notifcatie van DigiD was op 21 augustus 2020. Een volledig overzicht van genotificeerde eID-schema's is beschikbaar op de website van de Europese Commissie.[28] Inlogmiddelen die eIDAS-genotificeerd zijn en voldoen aan de eisen van het wetsvoorstel, kunnen in principe direct na inwerkingtreding van dit wetsvoorstel worden gebruikt.

De leden van de GroenLinks-PvdA-fractie vragen in welke gevallen een PersonIdentifier kan worden omgezet tot BSN dat bruikbaar is voor authenticatie via het Dezi-register.

Om de PersonIdentifier om te kunnen zetten in een BSN, moet de zorgmedewerker in de Basisregistratie Personen (BRP) of in de Registratie Niet-Ingezetenen (RNI) zijn geregistreerd. Alleen dan kan een BSN aan die zorgmedewerker worden gekoppeld of worden opgehaald via het BSN-koppelregister.

3. Verhouding tot hoger recht

3.1 eIDAS-verordening

De leden van de PVV-fractie willen graag weten hoe deze wet zich verhoudt tot bestaande Europese wetgeving, zoals de eIDAS-verordening? Wat is het doel om de zorg compatibel te maken met deze Europese richtlijn ?

Het wetsvoorstel is in lijn met Europese regels, zoals de eIDAS-verordening en de AVG. Zo zijn de eisen voor erkenning van inlogmiddelen gebaseerd op de eIDAS-normen. Dit geldt voor middelen die worden erkend onder de Wdo, door de eIDAS-verordening en voor erkenning op basis van de NEN 7518. De

[28] Europese Commissie, *Overview of pre-notified and notified eID schemes under eiDAS*.

architectuur van het Dezi-stelsel is in lijn met de eIDAS-referentiearchitectuur. De eis in het wetsvoorstel voor het verplicht toepassen van betrouwbaarheidsniveau hoog komt voort uit de AVG.

De eIDAS-verordening is geen richtlijn, maar een verordening. Een verordening is verbindend in al haar onderdelen en is rechtstreeks van toepassing in Nederland.[29] De eIDAS-verordening is de basis voor betrouwbare digitale dienstverlening in de EU. Het schrijft gemeenschappelijke eisen voor aan elektronische identificatie- en authenticatie die het veilig gebruik en inloggen bij overheidsinstanties en de private sector in de EU mogelijk moeten maken. Met het volgen en toepassen van deze verordening in de zorg worden onder andere de eisen nageleefd over betrouwbaarheidsniveaus, erkende inlogmiddelen en vertrouwensdiensten.

De leden van de PVV-fractie vragen of de regering kan toezeggen dat dit geen opmaat is naar een Europese digitale identiteit?

De Nederlandse zorgidentiteit is niet bedoeld als onderdeel van een Europese digitale identiteit voor burgers. De zorgidentiteit, zoals beschreven in het wetsvoorstel, is specifiek bedoeld voor zorgmedewerkers in Nederland en wordt gebruikt voor de identificatie en authenticatie van zorgmedewerkers binnen zorginformatiesystemen en gegevensuitwisselingssystemen. De zorgidentiteit kan daarom niet worden gebruikt voor andere doelen of publieke diensten, zoals die van de gemeente of de belastingdienst.

De leden van de PVV-fractie vragen waarom niet is gekozen voor doorontwikkeling van het UZI-register en UZI-middelen.

Het huidige UZI-stelsel behoeft verbetering op essentiële punten die niet met een doorontwikkeling zijn te ondervangen. Zo sluiten de huidige UZI-middelen niet goed aan op alle zorgprocessen. Ze werken bijvoorbeeld niet goed bij ambulant werk of op mobiele apparaten. Ook worden UZI-middelen als duur ervaren. Daarnaast zijn UZI-middelen niet flexibel. Een voorbeeld hiervan is dat bij een verandering in de werkrelatie of in de beroepsbevoegdheid een nieuw middel moet worden aangeschaft. Tot slot voldoen veel inlogmiddelen die momenteel in de zorg worden gebruikt niet aan het betrouwbaarheidsniveau hoog. Om die reden is gekozen voor de ontwikkeling van het Dezi-stelsel.

De leden van de PVV-fractie vragen, gezien het doel van de eIDAS-verordening om grensoverschrijdend inloggen mogelijk te maken, of het idee is om grensoverschrijdend te gaan werken ten grondslag ligt aan het wetsvoorstel.

De zorgidentiteit, zoals voorzien in het wetsvoorstel, is bedoeld voor zorgmedewerkers en vormt het middel waarmee zij zich op een betrouwbare en gestandaardiseerde wijze kunnen identificeren en authentiseren bij toegang tot zorginformatiesystemen en gegevensuitwisselingsvoorzieningen. Deze voorziening draagt bij aan veilige en doelmatige zorgverlening binnen Nederland, maar speelt ook een rol in de grensoverschrijdende context.

Wanneer een patiënt of cliënt uit een andere EU-lidstaat in Nederland zorg ontvangt, kan de zorgverlener met gebruik van zijn of haar zorgidentiteit, in lijn met de EHDS, toegang krijgen tot relevante medische gegevens uit het land van herkomst van de patiënt. Dit verloopt via het Nationaal Contactpunt voor eHealth (NCPeH), dat door Nederland wordt beheerd en aangeboden via het CIBG.

Om dit goed juridisch te borgen, wordt momenteel een wetsvoorstel voorbereid wat vlak voor het zomerreces een advies van de Afdeling advisering van de Raad van State heeft ontvangen.[30] Hiermee wordt verzekerd dat de zorgidentiteit ook in grensoverschrijdende situaties rechtmatig en effectief kan worden ingezet, uitsluitend ten behoeve van de directe zorgverlening aan de betreffende patiënt. Het doel hiervan is om de continuïteit en kwaliteit van zorg te ondersteunen, ook wanneer het landsgrenzen overstijgt.

3.2 Verhouding tot het vrij verkeer van goederen en diensten

De leden van de GroenLinks-PvdA-fractie erkennen het belang van veilige uitwisseling van data in de zorg. Houdt de regering er rekening mee dat de definitie van «passend beveiligd» zoals de AVG voorschrijft, in de toekomst

[29] Artikel 288 Verdrag betreffende de werking van de Europese Unie.
[30] Advies van de Afdeling advisering van de Raad van State van 2 juli 2025 (W13.25.00083/III).

kan veranderen? Houdt de regering bijvoorbeeld rekening met het toepassen van kwantumcryptografie als veiligheidsmaatregel in de toekomst?

De regering houdt rekening met het feit dat 'passend beveiligd' in de toekomst kan veranderen en dat in de toekomst kwantumcryptografie kan worden toegepast. Daar is namelijk mee rekening gehouden door geen technisch inhoudelijke eisen te stellen en te verwijzen naar normenkaders.

De leden van de GroenLinks-PvdA-fractie zijn benieuwd wat wordt bedoeld met «de afkomst» van een inlogmiddel. Doelt de regering hierop op het land van afkomst? Deelt de regering de mening dat de voorkeur uit moet gaan naar inlogmiddelen van Nederlandse en Europese leveranciers, om de strategische afhankelijkheden van niet-Europese grootmachten in vitale sectoren te verminderen?

Met 'de afkomst' van een middel wordt verwezen naar het kader, zoals het Wdo, PKIoverheid, de eIDAS-verordening of de NEN 7518 van waaruit het inlogmiddel is erkend.

De continuïteit van zorg mag op geen enkel moment afhankelijk worden van een klein aantal of uitsluitend niet-Europese technologiebedrijven, zeker tegen de achtergrond van een veranderende geopolitieke context. Het wetsvoorstel geeft een grondslag om inlogmiddelen aan te bieden die worden erkend door vier verschillende kaders: namelijk Wet digitale overheid, PKIoverheid, de eIDAS-verordening en de NEN 7518. Hierdoor kunnen ICT-leveranciers via verschillende routes hun middelen aanbieden.

Deze kaders stellen eisen en vragen om een officiële erkenning. Deze erkenning gebeurt door de Nederlandse overheid (op basis van de Wet digitale overheid en de PKIoverheid), op EU-niveau (bij de eIDAS-verordening), of door te voldoen aan de NEN-7518 (via een certificaat uitgegeven door een certificerende instelling onder de Raad van Accreditatie). Zowel de Wet digitale overheid als de NEN 7518 verwijzen naar de eIDAS-verordening.

Dit alles betekent dat alleen inlogmiddelen kunnen worden gebruikt die zijn erkend door de Nederlandse overheid of die onder toezicht staan van de Europese Unie. Daarnaast schrijft de eIDAS-verordening voor dat een verlener van vertrouwensdiensten in de EU gevestigd hoort te zijn, een vestiging heeft in de EU, of gevestigd zijn in een derde land dat een overeenkomst heeft gesloten met de EU op grond van artikel 218 VWEU.[31] Ook moeten verleners van vertrouwensdiensten onder toezicht staan van een nationale toezichthouder in een EU-land.

Daarmee wordt uitsluitend gebruik gemaakt van door Nederland erkende en/of onder Europese toezicht staande inlogmiddelen, zodat de continuïteit in de zorg in geen enkel geval volledig afhankelijk wordt van niet-Europese tech-leveranciers.

4. Verhouding tot nationale wetgeving

4.1 Aanpassing Wabvpz en Jeugdwet

De leden van de PVV-fractie vragen of er voldoende rekening wordt gehouden met bestaande nationale wetgeving, zoals de AVG?

Bij het voorstel is zorgvuldig rekening gehouden met de bestaande nationale wetgeving. Het sluit ook goed aan bij bijvoorbeeld de eisen van passende technische beveiligingsmaatregelen van Europese regelgeving zoals de AVG. Er wordt immers ingelogd op het hoogste betrouwbaarheidsniveau, zoals de AVG voorschrijft aangezien er sprake is van gevoelige persoonsgegevens.[32]

De leden van de GroenLinks-PvdA-fractie vragen de regering om beter te duiden wat er praktisch verandert doordat «in vervolg ook zorgmedewerkers die werkzaam zijn voor een zorgaanbieder zich in het register [kunnen] laten inschrijven.» Hoe is dit anders dan de huidige situatie, en waarom is dit een verbetering?

Het huidige register is een register van zorgaanbieders, ofwel instellingen en solistisch werkende zorgverleners. Zij kunnen zich inschrijven als abonnee en kunnen voor zichzelf en/of hun medewerkers

[31] Artikelen 2,14 en 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 (*PbEU 2014,* L257/73).

[32] Artikel 5, eerste lid, sub f en artikel 32 van de Algemene verordening gegevensbescherming en brief Autoriteit Persoonsgegevens d.d. 4 oktober 2018 met kenmerk z2018-17577 en Kamerstukken II 2016-2017, 27 529, nr. 143, blz. 1.

UZI-middelen aanschaffen. De medewerkers met een UZI-middel staan dan als middelenhouder geregistreerd onder de abonneeregistratie. Niet alle UZI-middelen kunnen voor elke groep medewerkers worden aangeschaft. Zo kan de zorgverlenerspas alleen worden gebruikt door een zorgverlener met een BIG-registratie.

In het nieuwe register hebben medewerkers een eigen, unieke registratie die gekoppeld kan worden aan zorgaanbieder(s). De zorgaanbieder bepaalt welke autorisaties nodig zijn op basis van de rol van de zorgmedewerker. De keuze voor een inlogmiddel is vrij binnen de mogelijkheden die het Dezi-stelsel biedt. Dit is dus een meer flexibele optie voor zorgmedewerkers dan het huidige UZI-register.

De leden van de GroenLinks-PvdA-fractie vragen hoeveel meer mensen door de aanpassingen in dit wetsvoorstel kunnen worden toegevoegd aan het Dezi-register en daarmee ook toegang krijgen tot de zorggegevens van patiënten?

In principe kan iedereen die valt onder de definitie van zorgmedewerker een registratie aanvragen voor het Dezi-register. Dit sluit aan bij de vereisten uit verschillende wet- en regelgeving om de gegevens van de patiënt beter te beveiligen en om interoperabiliteit te voorzien, zodat gegevens van de patiënt uitgewisseld kunnen worden. In de zorg zijn volgens het CBS circa 1,5 miljoen mensen werkzaam.

Een registratie in het Dezi-register betekent echter niet dat er direct toegang verkregen kan worden tot zorggegevens van patiënten/cliënten. Een medewerker moet tevens beschikken over een werkrelatie, een goedgekeurd inlogmiddel en daarnaast toegang hebben tot het systeem van een zorgaanbieder.

De leden van de GroenLinks-PvdA-fractie vragen of er, naast de genoemde Besluiten en Regeling, ook wijzigingen in andere delen van de sectorale wetgeving zijn overwogen. Hoe is de regering tot de conclusie gekomen dat alleen de voorgestelde wijzigingen noodzakelijk zijn?

Er zijn geen wijzigingen van andere delen van sectorale wetgeving overwogen. Het voornemen was altijd om bij een wijziging te richten op besluiten en regels die zien op SBV-z en om de regelingen over inlogmiddelen aan te passen. Vandaar dat dit wetsvoorstel en de onderliggende regelgeving zich altijd heeft toegespitst op de Wabvpz, de Jeugdwet en het Besluit Jeugdwet.

De voorgestelde wijzigingen zijn gekozen met het oog op de doelstellingen van het wetsvoorstel samen met het uitgangspunt om wijziging van wetten tot een minimum te beperken. Hierom worden alleen hoofdstuk 3 van de Wabvpz en artikelen 7.2.7 en 7.2.8 van de Jeugdwet aangepast. Daarmee worden de kerndoelen van dit wetsvoorstel bereikt, zoals het mogelijk maken van het Dezi-register en het kunnen gebruiken van verschillende inlogmiddelen.

4.2 Verhouding met de Wdo

De leden van de GroenLinks-PvdA-fractie vragen de regering om duidelijk te maken welke inlogmiddelen de voorkeur hebben voor gebruik in de zorg. Ziet de regering voordelen en nadelen aan het gebruik van Wdo-middelen ten opzichte van andere toegestane middelen? Zo ja, hoe stimuleert regering het gebruik van middelen die volgens haar de meeste voordelen bieden?

De regering heeft geen voorkeur voor bepaalde middelen vanuit een specifiek normenkader. In plaats daarvan bied ik met dit wetsvoorstel juist ruimte voor het gebruik van verschillende soorten middelen. Er worden geen duidelijke voor- of nadelen gezien van de Wdo-middelen in vergelijking met andere middelen die zijn toegestaan. Ook is er geen beleid of maatregel opgenomen die het gebruik van bepaalde middelen specifiek gaat stimuleren.

Wel moet worden opgemerkt dat het Wdo-middel DigiD niet speciaal is gemaakt voor gebruik in de zorg. DigiD is vooral bedoeld voor communicatie tussen burgers en de overheid. In de zorg zijn de werkprocessen anders en stellen ze specifieke eisen. Zorgmedewerkers moeten bijvoorbeeld heel snel kunnen inloggen wanneer ze van werkplek kunnen wisselen, zeker als ze ambulant werken. Ook zijn er vaak extra regels voor hygiëne waardoor zorgspecifieke middelen beter aansluiten op deze situaties. Dat betekent niet dat het Wdo-middel DigiD niet bruikbaar is in de zorg, dat bleek bijvoorbeeld uit de positieve ervaringen in de pilot met een aantal huisartsen.[33] Onder de Wdo kunnen ook andere middelen worden

[33] CIBG, '*Positieve tussentijdse resultaten SBV-Z pilot voor Dezi'*, *18 februari 2025*.

erkend die, net als DigiD, in bepaalde zorgprocessen prima werken. Vandaar dat er geen voorkeur is voor bepaalde middelen en dat het gebruik van een specifiek middel niet wordt gestimuleerd.

4.3 Verhouding met de Wegiz

De leden van de GroenLinks-PvdA-fractie vragen om een onderbouwing dat het voldoen aan de NEN-norm voor identificatiemiddelen niet noodzakelijk is. Heeft de regering dit wel overwogen?

In het wetsvoorstel zijn er vier mogelijkheden om op het Dezi-stelsel aan te sluiten als identificatiemiddel. Dit kan met middelen erkend door de Wdo, middelen erkend vanuit de eIDAS-verordening, PKIo-servicecertificaten en zorgspecifieke middelen. De middelen die onder de Wdo en eIDAS zijn erkend en die daarnaast betrouwbaarheidsniveau hoog hebben, kunnen worden gebruikt binnen het Dezi-stelsel. Voor PKI-o-servicecertificaten erkend op betrouwbaarheidsniveau hoog geldt hetzelfde. Echter, voor middelen specifiek ontwikkeld onder de NEN-norm 7518 is dit anders. Deze middelen horen te worden gecertificeerd conform de NEN-norm 7518.

De leden van de GroenLinks-PvdA-fractie vragen hoe het ook toestaan van inlogmiddelen onder de Wdo of het PKI-overheidsstelsel administratieve lasten beperkt.

Het toestaan van Wdo-erkende en PKIoverheid-gebaseerde inlogmiddelen binnen het Dezi-stelsel verlaagt de administratieve lasten voor zorgaanbieders. Zorgaanbieders en zorgmedewerkers die al gebruikmaken van Wdo-erkende middelen, zoals DigiD, kunnen die ook inzetten voor toegang tot zorginformatiesystemen, mits ze voldoen aan het vereiste betrouwbaarheidsniveau. Dit voorkomt dubbele registratie en de aanschaf van nieuwe middelen.

5. Toezicht en handhaving

De leden van de PVV-fractie vragen welke instantie verantwoordelijk is voor het toezicht op de implementatie van de digitale identificatie.

Het toezicht op de implementatie en naleving van de verplichtingen rond digitale identificatie in de zorg is belegd bij de IGJ. De IGJ ziet toe op het gebruik van erkende inlogmiddelen op betrouwbaarheidsniveau hoog, de aansluiting van zorgaanbieders op het Dezi-stelsel en het adequaat organiseren van veilige digitale toegang tot cliëntgegevens. Samen met deze nota naar aanleiding van het verslag, wordt ook een nota van wijziging meegestuurd. Hierin worden de taken van de IGJ verder ingevuld en vormgegeven in het kader van dit wetsvoorstel en van de Verzamelwet gegevensverwerking II.a, die een paragraaf in de Wabvpz toevoegt over toezicht- en handhaving.

De leden van de PVV-fractie vragen hoe wordt gewaarborgd dat zorgaanbieders ook daadwerkelijk tijdig voldoen aan de eisen die in het wetsvoorstel worden gesteld.

Om te waarborgen dat zorgaanbieders tijdig aan de eisen voldoen, hanteert de regering een combinatie van een gefaseerde overgangstermijn voor UZI-gebruikers tot uiterlijk 1 januari 2029, een actieve monitoring van de voortgang door het CIBG met terugkoppeling naar het ministerie van VWS en een gerichte ondersteuning voor zorgorganisaties, onder andere via handreikingen en pilots.

Het uitgangspunt is dat ondersteuning en begeleiding centraal staan tijdens de implementatiefase, maar dat bij uitblijvende actie ook handhavend door de IGJ kan worden opgetreden om de veiligheid van patiëntgegevens te borgen.

De leden van de GroenLinks-PvdA-fractie vragen of de minister kan onderbouwen dat er genoeg middelen aan de IGJ worden toebedeeld om de wet uit te voeren. Deze vragen of de IGJ heeft bevestigd dat zij adequaat zijn ondersteund om toe te zien en waar nodig te handhaven op het gebruik van de juiste inlogmiddelen?

De IGJ heeft bevestigd dat zij voldoende expertise en kennis heeft om de toebedeelde taken uit te voeren. Uitgaand van een risico-gestuurde aanpak verwacht de IGJ over voldoende middelen te beschikken voor het uitvoeren van de toezicht- en handhavingstaken. De IGJ merkt hierbij op dat dit anders kan zijn als zij een hoog aantal meldingen zal ontvangen. De IGJ voert namelijk, naast risico-gestuurd toezicht, ook incidententoezicht uit. Bij dit laatste soort toezicht reageert de IGJ op meldingen en klachten van burgers, zorgaanbieders, fabrikanten, gemeenten en andere instanties over incidenten, misstanden en

terugkerende tekortkomingen. De IGJ verwacht niet dat het aantal meldingen vanwege dit wetsvoorstel stijgt.

De leden van de GroenLinks-PvdA-fractie delen de zorgen over het scenario dat, door het intrekken van goedkeuring van inlogmiddelen of het blijven gebruiken van UZI-middelen nadat de wettelijk toegestane termijn is verstreken, de kwaliteit van zorg in gevaar komt. Zij vragen de regering om beter uit te leggen wat zij van de IGJ verwacht in het geval dit dreigt te gebeuren.

Voor de regering staan zowel de continuïteit als de kwaliteit van de zorgverlening voorop. In een individuele belangenafweging over de genoemde besluiten komt het waarborgen van de continuïteit van de zorgverlening en de kwaliteit van de zorg een groot gewicht toe. De intrekking van de goedkeuring van een inlogmiddel gebeurt door de CIBG namens de minister. Hierbij kan de IGJ ondersteunen door een inschatting te maken van hoe de intrekking van het middel de kwaliteit van de zorg kan beïnvloeden.

De leden van de GroenLinks-PvdA-fractie vragen hoe de IGJ zorgaanbieders kan dwingen om hun inlogmiddelen te vervangen.

Zowel bij de intrekking, als het blijvend gebruik van UZI-middelen bestaat de ondersteunende rol van de IGJ uit de mogelijkheid om haar bevoegdheden in te zetten om te bewerkstelligen dat de betreffende zorgaanbieder informatie verschaft en/of om hem ertoe te bewegen maatregelen te treffen om de inlogmiddelen te vervangen. Dit kan bijvoorbeeld door met deze zorgaanbieder in

gesprek te gaan of verbeterpunten op te leggen. In het uiterste geval kan de IGJ overgaan tot het geven van een schriftelijke aanwijzing, een schriftelijk bevel of het opleggen van een herstelsanctie, zoals een last onder dwangsom.

De leden van de GroenLinks-PvdA-fractie vragen wat de precieze definitie is van de «ondersteunende rol» die de regering van de IGJ verwacht.

De ondersteunende rol van de IGJ bestaat uit de mogelijkheid een inschatting te maken van hoe intrekking van een inlogmiddel de kwaliteit van zorg kan beïnvloeden. De IGJ kan haar bevoegdheden inzetten om van een betreffende zorgaanbieder informatie te verkrijgen of om hem ertoe te bewegen maatregelen te treffen om inlogmiddelen te vervangen. Dit kan bijvoorbeeld door met deze zorgaanbieder in dialoog te gaan of door verbeterpunten aangeven. In het uiterste geval kan de IGJ overgaan tot het opleggen van een schriftelijke aanwijzing, een schriftelijk bevel of het opleggen van een herstelsanctie, zoals een last onder dwangsom

De leden van de GroenLinks-PvdA-fractie vragen of voor de regering het waarborgen van de continuïteit van zorgverlening voorop staat, en wat wordt gedaan als een zorgaanbieder niet tijdig overstapt naar een gecertificeerd inlogmiddel en een geforceerde overstap de zorgverlening tijdelijk zou belemmeren?

Het waarborgen van de continuïteit van de zorg is leidend. Ik acht de kans dat een zorgaanbieder UZI-middelen blijft gebruiken klein. Zorgaanbieders worden immers reeds nu al uitgebreid geïnformeerd over de overstap naar het Dezi-stelsel, de verplichtstelling van de inlogmiddelen die onder dit stelsel gelden en over het feit dat vanaf 1 januari 2029 de UZI-middelen niet meer bruikbaar zijn.

De leden van de GroenLinks-PvdA-fractie vragen waar zorgaanbieders zich kunnen melden met vragen over deze overstap naar Dezi, en waar zij terecht kunnen voor ondersteuning.

Zorgaanbieders kunnen zich met vragen en verzoeken tot ondersteuning primair wenden tot de implementatieorganisatie Dezi. Om deze overstap zo soepel mogelijk te laten verlopen is de website www.dezi.nl beschikbaar voor het vervullen van een eerste informatiebehoefte. Daarnaast zijn en worden er diverse informatiesessies georganiseerd die open staan voor geïnteresseerde zorgaanbieders. Naast de focus op zorgaanbieders wordt er vanuit het ministerie ook gewerkt met een klankbordgroep bestaande uit vertegenwoordigers van koepel- en brancheorganisaties. Ook worden er bijeenkomsten voor ICT-leveranciers georganiseerd om deze overstap in samenhang te benaderen.

De leden van de GroenLinks-PvdA-fractie vragen hoe de minister de verwachting kan onderbouwen dat dit weinig voor zal komen.

Gezien de variëteit aan zorgaanbieders en de mate waarin en de wijze waarop automatisering geregeld is, is het moeilijk om precies te zeggen hoe snel de overgang naar het Dezi-stelsel kan plaatsvinden. Er is geen eenduidig antwoord, omdat elke zorgaanbieder verschillende stappen zal moeten zetten op basis van hun huidige situatie en automatiseringsniveau.

Om zorgaanbieders te ondersteunen in deze overgang, is er een gefaseerde aanpak voorzien. De huidige UZI-passen en de nieuwe middelen uit het Dezi-stelsel zullen een periode naast elkaar bestaan. Dit zorgt ervoor dat zorgaanbieders de tijd hebben om oude inlogmiddelen geleidelijk te vervangen, terwijl ze tegelijkertijd de patiëntenzorg kunnen blijven ondersteunen met zowel de oude als de nieuwe inlogmiddelen.

Het Dezi-systeem zelf is zo ingericht dat zorgaanbieders maar één technisch koppelvlak hoeven te realiseren om toegang te krijgen tot alle erkende Dezi-inlogmiddelen. Dit maakt de integratie eenvoudiger, omdat alle middelen via hetzelfde koppelvlak kunnen worden gebruikt.

Zorgmedewerkers kunnen zichzelf op voorhand al registreren in het Dezi-register. Zodra de zorgaanbieder bevestigt dat er een werkrelatie is, kan de zorgmedewerker direct inloggen met een erkend Dezi-inlogmiddel. Dit maakt dat de overstap door de zorgaanbieder wordt bepaald.

Om ervoor te zorgen dat de overgang soepel verloopt, heeft het CIBG een teststraat opgezet voor de relevante technische koppelingen van het Dezi-systeem. Zorgaanbieders en hun leveranciers kunnen deze teststraat gebruiken om alles grondig te testen voordat ze daadwerkelijk de overstap maken. Zodra een zorgaanbieder klaar is met de voorbereiding en het testen, kunnen ze de overstap naar het Dezi-systeem maken. Tot 1 januari 2029 kunnen ze echter nog steeds de UZI-middelen gebruiken naast de nieuwe Dezi-middelen.

Deze aanpak biedt zorgaanbieders voldoende tijd en middelen om zich goed voor te bereiden op de overstap, zodat de overgang naar het Dezi-systeem op een gecontroleerde en efficiënte manier kan plaatsvinden terwijl de patiëntenzorg gecontinueerd wordt.

De leden van de VVD-fractie lezen dat de Minister van VWS over kan gaan tot intrekking van de goedkeuring van een middel indien het middel onveilig blijkt. Zij vragen op welke manier de veiligheid van middelen wordt beoordeeld. In hoeverre zijn gesimuleerde hacks onderdeel van dit proces zoals dit in de financiële sector gebeurt?

Organisaties die middelen uitgeven moeten aantoonbaar voldoen aan strenge (veiligheids-)eisen vanuit het eIDAS-normenkader. Een onderdeel hiervan is het verplicht uitvoeren van een penetratietest evenals het uitvoeren van scans op kwetsbaarheden. Het inlogmiddel zelf moet aan diverse certificeringen en security assessments voldoen die onder de eIDAS-verordening worden vereist.

De leden van de NSC-fractie hechten grote waarde aan de rol die de AP speelt in het toezien op de wettelijke regels van het beschermen van persoonsgegevens. Welke rol speelt de AP concreet in de handhaving van het beschermen van persoonsgegevens bij dit voorstel?

De handhaving op de naleving van de wettelijke verplichtingen rond het gebruik van het Dezi-register en erkende inlogmiddelen is belegd bij de IGJ. De IGJ ziet toe op de juiste toepassing van veilige identificatie en authenticatie in de zorg, binnen het bredere kader van verantwoorde gegevensuitwisseling.

De rol van de AP wordt niet verder uitgebreid. Zij gaat haar gebruikelijke taken op het gebied van gegevensbescherming blijven uitvoeren, zoals in actie komen bij datalekken. Hiervan kan sprake zijn bij het verlies of misbruik van een inlogmiddel. Ik benadruk hierbij dat het stelsel sterke technische en organisatorische waarborgen biedt, zoals directe intrekking, logging en sterke authenticatie, zodat persoonsgegevens goed beschermd en de risico's beheersbaar zijn. Zoals ook aangegeven in de beantwoording bij Verzamelwet gegevensverwerking VWS II.a, waar het toezicht van de IGJ in de Wabvpz is uitgewerkt, zijn al samenwerkingsafspraken gemaakt tussen de IGJ en de AP. Dit wetsvoorstel sluit daarbij aan.

De leden van de NSC-fractie vragen wat de mogelijke gevolgen zijn van verlies of misbruik van het nieuwe inlogmiddel?

Het verlies van een inlogmiddel hoeft niet direct gevolgen te hebben. De goedgekeurde inlogmiddelen uit het Dezi-stelsel moeten voldoen aan betrouwbaarheidsniveau hoog, wat betekent dat zeer hoge eisen zijn gesteld aan de beveiliging van een inlogmiddel.

Onderdeel van deze beveiliging is dat voor het daadwerkelijk 'authentiseren' gebruik gemaakt moet worden van minimaal twee verschillende categorieën van authenticatiefactoren. Authenticatiefactoren zijn kennis: iets dat je weet (bijvoorbeeld een pincode), bezit: iets dat hebt (bijvoorbeeld een Smartcard) of inherentie: iets dat je bent (bijvoorbeeld een vingerafdruk). Daarbij geldt dan ook nog de eis dat beide factoren onafhankelijk (van elkaar) zijn en een hoge mate van zekerheid moeten bieden. Dit betekent dat bij verlies van bijvoorbeeld een mobiele telefoon met daarop een ID-wallet applicatie, ook bijvoorbeeld een pincode, vingerafdruk of face-id nodig is als tweede (of zelfs derde) authenticatiefactor voor het daadwerkelijke gebruik. Om gebruik te kunnen maken van een inlogmiddel moet een ongeoorloofde gebruiker dus niet alleen het inlogmiddel bemachtigen, maar ook nog de andere authenticatiefactor(-en).

Om risico's bij verlies verder te verkleinen, is het mogelijk inlogmiddelen direct in te trekken. Daarmee zijn deze inlogmiddelen per direct onbruikbaar binnen het Dezi-stelsel. Deze intrekking wordt gefaciliteerd door het CIBG als onderdeel van de (beoogde) dienstverlening. Daarnaast geldt vanuit de eIDAS-verordening een verplichting voor een leverancier van vertrouwensdiensten om een intrekkingsfunctionaliteit voor inlogmiddelen aan te bieden. Hierdoor is er dus een dubbel vangnet.

De leden van de CDA-fractie lezen dat bij of krachtens algemene maatregel van bestuur regels kunnen worden gesteld aan het intrekken van goedkeuring voor een inlogmiddel. Deze leden vragen of de verantwoordelijkheid hiervoor bij de Minister ligt of bij de Inspectie en wie hierin precies welke rol heeft.

Ik ben verantwoordelijkheid voor de intrekking van de goedkeuring van een inlogmiddel. Het CIBG voert het namens mij uit.

De leden van de CDA-fractie vragen of de regering voornemens is zulke nadere regels in een algemene maatregel van bestuur vast te leggen en zo ja, aan welke nadere regels de regering denkt. Deze leden vragen ook of de regering overweegt om regels te stellen op het gebied van het borgen van de nationale veiligheid of de strategische autonomie.

De regering is voornemens nadere regels voor de intrekking in een algemene maatregel van bestuur uit te werken. De regels hierin zien op de gevallen waarin een goedkeuring van een inlogmiddel wordt geschorst of ingetrokken. Bij een schorsing stopt de goedkeuring tijdelijk. Een goedkeuring kan worden ingetrokken bij aanhoudende problemen. Hiervan kan sprake zijn wanneer deze problemen de betrouwbaarheid van het Dezi-stelsel blijvend in gevaar brengen.

In dit wetsvoorstel liggen geen mogelijkheden om nadere regels te stellen met het oog op de nationale veiligheid en strategische autonomie. In dat geval zullen deze eisen, indien nodig, opgenomen moeten worden in de Wdo, de eIDAS-verordening of de NEN 7518.

6. Gegevensbeschermingseffectbeoordeling

Voor de leden van de NSC-fractie is het van groot belang dat bij gevoelige persoonsgegevens data zoveel mogelijk lokaal wordt opgeslagen. Is de dataopslag van het Dezi-register lokaal geregeld? Zo nee, hoe is de dataopslag dan georganiseerd?

De data van het Dezi-register wordt lokaal, binnen Nederlandse staatsgrenzen, versleuteld opgeslagen.

6.1 Authenticatieverklaringen CIBG

De leden van de GroenLinks-PvdA-fractie ontvangen graag meer informatie over de versleuteling die plaatsvindt in het ophalen van de BSN. Is data te allen tijde end-to-end versleuteld? Op welke momenten in het proces worden gegevens ontsleuteld?

Op basis van tweezijdige authenticatie is er sprake van een versleutelde verbinding waardoor de data *end-to-end* versleuteld is. Ontsleuteling vindt plaats op het moment dat het verzoek is ontvangen om het BSN om te zetten naar een Dezi-nummer.

De leden van de GroenLinks-PvdA-fractie vragen of nader kan worden toegelicht hoe de informatiehuishouding en databeveiliging van het CIBG zijn ingericht?

De inrichting van de informatiehuishouding en de beveiliging van data bij het CIBG is een veelomvattend pakket aan maatregelen. Hierbij kan gedacht worden aan: beveiligde omgevingen met meerdere lagen voor toegangsbeveiliging, versleuteling van databases, versleuteling van berichten, gescreend personeel, access management.

Er wordt geen onderscheid gemaakt tussen de verschillende beveiligingsniveaus en de mate van beveiliging. Het CIBG dient als implementerende partij alle niveaus te ondersteunen. Deze eis staat beschreven in de eIDAS-verordening.[34] In dit verband is er dus geen sprake van specifieke privacy bevorderende standaarden, omdat die al standaard toegepast moeten worden ook bij lagere beveiligingsniveaus. Bij andere producten van het CIBG is het zo ook al geïmplementeerd (bijvoorbeeld het gebruik van DigiD bij het Donorregister). Hoewel het grootste gedeelte van de gebruikers DigiD Substantieel gebruikt, moet het Donorregister ook DigiD Hoog kunnen ondersteunen. Het is namelijk aan de gebruiker om te kiezen met welk veiligheidsniveau die wil inloggen. Het CIBG wordt jaarlijks geaudit op het voldoen aan de DigiD-eisen voor elk product dat DigiD aanbiedt. Jaarlijkse terugkerende audits voor het Dezi-register geven de verifieerbare waarborgen dat de Dezi-functie geboden wordt volgens de voorschriften.

De leden van de GroenLinks-PvdA-fractie vragen welke privacy bevorderende standaarden vallen onder het betrouwbaarheidsniveau hoog?

Binnen het Dezi-register worden waar mogelijk *Privacy Enhancing Techniques* (PET's) toegepast. De AVG verplicht organisaties daarnaast *Privacy by Design* toe te passen en om op basis van een risicoanalyse passende maatregelen te nemen voor de beveiliging van persoonsgegevens. Daarbij moet rekening worden gehouden met de stand van de techniek.

Om risico's te verminderen worden er verschillende PET's ingezet. Bij het CIBG worden voor het Dezi-register verschillende PET's toegepast die vallen onder het betrouwbaarheidsniveau hoog. Allereerst worden er zogenoemde 'algemene PET-maatregelen' meegenomen, zoals het toepassen van een authenticatie- en autorisatiemanagement voor de toegang tot gegevens van het Dezi-register. Ook het ontwikkelen van een logging- en monitoringbeleid maakt onderdeel uit van de implementatie van Dezi. Daarnaast wordt, zoals hierboven aangegeven, berichtuitwisseling gerealiseerd met berichtencryptie. Ook is er gekozen om te werken met koppelingen met authentieke bronnen om zo de gegevens bij de bron te kunnen laten.

De leden van de GroenLinks-PvdA-fractie vragen of is overwogen om aanvullende privacy bevorderende technieken toe te passen? Deze leden zijn benieuwd hoe de regering het principe van dataminimalisatie, dat volgt uit de AVG, heeft toegepast in de inrichting van dit systeem.

Aanvullende technieken zijn overwogen. Echter, de maatregelen die genomen zijn, geven al voldoende invulling aan de geldende regelgeving. Bovendien is gekozen te werken met koppelingen met authentieke bronnen, om zo de gegevens bij de bron te kunnen laten. Hiermee wordt het principe van dataminimalisatie toegepast.

De leden van de GroenLinks-PvdA-fractie zijn benieuwd hoe en waar de «logging»-gegevens worden opgeslagen, en hoe wordt toegezien op de bewaartermijnen die hiervoor gelden? Onder welke voorwaarden kunnen logging-gegevens worden opgevraagd, en door wie? Na welke bewaartermijn dienen zij te worden verwijderd ?

De logging-gegevens worden lokaal, binnen Nederlandse staatsgrenzen, opgeslagen. Binnen het Dezi-register worden verschillende typen logging-gegevens vastgelegd. De bewaartermijn wordt vooraf bepaald per type log-gegeven. De logging-gegevens worden periodiek verwijderd op het moment dat de bewaartermijn verstreken is. Betrokkenen kunnen op basis van het inzagerecht van de AVG de logging-gegevens opvragen die op hun dossier van toepassing zijn.

[34] Artikelen 19 en 24 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).

6.2 Verwerken van het BSN door de middelenuitgever zorgspecifieke middelen

De leden van de GroenLinks-PvdA-fractie vragen waarom enkel het BSN voldoet als geschikt persoonsgegeven om een Dezi-nummer te koppelen aan een persoon. Zijn er andere mogelijkheden overwogen? Zo ja, waarom zijn deze niet gebruikt?

Wanneer iemand zich inschrijft in het Dezi-register, dan wordt het BSN gebruikt. Met het BSN kunnen de benodigde gegevens voor inschrijving in het Dezi-register automatisch worden ingevuld. Zo gaat het inschrijven sneller, makkelijker en op basis van brongegevens van de overheid. Ook helpt het BSN om te controleren of iemand bevoegd is om in de zorg te werken. Dit gebeurt volgens de regels van de Wet BIG. Heeft een zorgmedewerker een beroepsbevoegdheid conform Wet BIG, dan staat deze persoon in het BIG-register, dat in beheer is bij het CIBG. Daarbij is het BSN de sleutel tussen de registratie en de persoon.

De overheid gebruikt bij dit soort processen doorgaans het BSN. Dat is nodig, omdat het BSN een belangrijk onderdeel is van het stelsel van basisregistraties in Nederland. Dankzij het BSN hoeft de overheid geen gegevens op te vragen die al bekend zijn *('only once-principe'*). Dat voorkomt dubbel werk en fouten.

Het wetsvoorstel maakt mogelijk dat zorgaanbieders het BSN mogen gebruiken voor een specifieke taak. Dat is belangrijk, omdat het BSN een gedeeld kenmerk is tussen de overheid en de zorgaanbieder. Hierdoor kunnen zij samen zeker weten dat het om dezelfde persoon gaat. Als een zorgmedewerker een zorgspecifiek inlogmiddel nodig heeft, moet duidelijk zijn wie die persoon is om aan de zorgidentiteit gekoppeld te worden. De zorgaanbieder moet de identiteit controleren met een geldig identiteitsbewijs volgens de WID. Het BSN dat op of uit het identiteitsbewijs komt, kan dan worden gebruikt om deze persoon te koppelen aan zijn of haar gegevens in het Dezi-register. Dat maakt de controle betrouwbaar.

Er is ook gekeken naar een alternatief waarbij het BSN niet wordt gebruikt. In dat geval moeten andere en vooral meer gegevens van het identiteitsbewijs worden gebruikt om iemand te herkennen. Echter, is dit minder veilig en vergroot het de kans op fouten, zoals dat iemand wordt verward met een ander. Dat is een probleem, vooral als het gaat om het aanvragen van een digitale zorgidentiteit op het hoogste beveiligingsniveau. Zo'n persoonsverwisseling mag niet gebeuren. Daarom is het beter het BSN in deze context te gebruiken.

De leden van de GroenLinks-PvdA-fractie vragen op welke wijze het BSN na de eenmalige werking wordt gepseudonimiseerd, en kan de regering onderbouwen dat deze in geen enkel geval herleidbaar is naar een persoon?

Het BSN zal door een zorgaanbieder, die de uitgever is van een zorgspecifiek middel, eenmalig worden gebruikt om het Dezi-nummer op te halen uit het Dezi-register.

Na deze omwisseling wordt het Dezi-nummer door de middelenuitgever gekoppeld aan het zorgspecifieke middel. Daarna mag het BSN niet meer worden gebruikt voor dit doel en dient het op grond van de AVG uit de administratie, die ten behoeve van deze koppeling wordt gevoerd, te worden verwijderd. De eenmalige BSN-verwerking zal worden uitgevoerd door de zorg- of jeugdhulpaanbieder voor wie de betreffende medewerker werkzaam is.

Als een zorgmedewerker een zorgspecifiek middel gebruikt om in te loggen met een zorgidentiteit, is voor andere gebruikers van het stelsel alleen het Dezi-nummer te zien. Het zorgspecifieke middel en de zorgidentiteit bevatten geen BSN, enkel het Dezi-nummer. De zorgidentiteit kan door het CIBG worden herleid tot de identiteit van de persoon doordat het Dezi-register de vertaling Dezi-nummer - BSN kan maken.

Het CIBG wordt alleen voor de NEN 7518 geacht het BSN om te wisselen. Voor andere inlogmiddelen is dit niet nodig. Daarnaast kan de zorgidentiteit ook worden herleid door de zorgaanbieder waarvoor de medewerker werkzaam is. Op die zorgaanbieder rust immers ook de verplichting om te loggen welke medewerkers elektronische zorginformatiesystemen of uitwisselingssystemen raadplegen.

De leden van de GroenLinks-PvdA-fractie vragen om een nadere onderbouwing van de analyse dat een koppeling gemaakt door de zorgmedewerker zelf geen werkbare oplossing is. In hoeverre heeft de regering deze oplossing overwogen?

Een alternatieve oplossing is overwogen, maar het is als te riskant bevonden wanneer een zorgmedewerker zelf de koppeling maakt. Dit kan leiden tot persoonsverwisseling, of dat nu per ongeluk of opzettelijk gebeurt. Als dat gebeurt, kunnen er inlogmiddelen ontstaan die niet aan de juiste zorgmedewerker zijn gekoppeld. Dit maakt het systeem onbetrouwbaar, wat de veiligheid en de betrouwbaarheid van zorgprocessen in gevaar kan brengen.

Bovendien kunnen er problemen ontstaan als een zorgmedewerker zelf diens identiteitsmiddel registreert. Het kan lastig zijn dit proces goed uit te voeren zonder hulp. Mensen maken soms fouten bij het invoeren van gegevens of ze begrijpen niet altijd welke informatie nodig is voor een veilige registratie. Dit kan leiden tot onjuiste koppelingen, waardoor de persoon niet goed geïdentificeerd kan worden in het systeem.

Het bovenstaande wordt voorkomen door de taak in het HR-proces van de zorgaanbieder te beleggen. Hier worden (toch) al gegevens vastgelegd van de zorgmedewerker voor het vastleggen van de werkrelatie. De eisen vanuit bijvoorbeeld NEN7510 en NEN7513 zorgen dat hier goede processen en logging op toezien.

De leden van de NSC-fractie vragen de regering of Privacy Enhancing Techniques (PET's) worden toegepast binnen de standaarden van deze wetswijziging. Zo nee, is de regering dan alsnog bereid deze PET's binnen de standaarden van de wetswijziging toe te voegen?

De AVG verplicht organisaties om *Privacy by Design* toe te passen en om op basis van een risicoanalyse passende maatregelen te nemen voor de beveiliging van persoonsgegevens. Daarbij moet rekening worden gehouden met de stand van de techniek. Om risico's te verminderen worden er verschillende PET's ingezet.

Het uitgangspunt is *Privacy by Design*, dit kan leiden tot inzet van deze technologieën. Keuze voor technologie is aan zorgaanbieders en wetenschap. Het Ministerie van VWS ziet toe op naleving van toepassing van het uitgangspunt van *Privacy by Design*.

Waar VWS zelf verantwoordelijk is voor ontwikkeling van toepassingen in de zorg is *Privacy & Security by Design* ook het uitgangspunt.

Bij het CIBG worden voor het Dezi-register verschillende PET's toegepast. Allereerst worden er zogenoemde 'algemene PET-maatregelen' meegenomen, zoals het toepassen van een authenticatie- en autorisatiemanagement voor de toegang tot de gegevens van het Dezi-register. Ook het ontwikkelen van een logging- en monitoringbeleid maakt onderdeel uit van de implementatie van Dezi. Daarnaast wordt berichtuitwisseling gerealiseerd door middel van berichtencryptie. Ook is er gekozen te werken met koppelingen met authentieke bronnen, om zo de gegevens bij de bron te kunnen laten.

6.3 Vergelijkbaar met de Wdo

De leden van de GroenLinks-PvdA-fractie vragen hoe de regering ervoor zorgt dat een BSN-verwerking daadwerkelijk eenmalig plaatsvindt. Is het technisch onmogelijk om één BSN meermaals te verwerken?

Het BSN zal door de middelenuitgever eenmalig worden gebruikt om het Dezi-nummer op te halen uit het door de overheid beheerde Dezi-register. Na deze omwisseling wordt het Dezi-nummer door de middelenuitgever gekoppeld aan het zorgspecifieke middel. Daarna mag het BSN niet meer worden gebruikt ten behoeve van het genoemde doel en moet het worden verwijderd uit de administratie van de middelenuitgever.

De leden van de GroenLinks-PvdA-fractie vragen of na de eerste koppeling van een BSN aan een Dezi-nummer, datzelfde Dezi-nummer voorgoed is gekoppeld aan die ene medewerker.

Het is vanuit het Dezi-register bezien technisch mogelijk om één BSN meermaals te verwerken. Dat moet omdat een persoon met meer organisaties een werkrelatie kan hebben en het dus ook mogelijk is te beschikken over meerdere zorgspecifieke inlogmiddelen.

De leden van de GroenLinks-PvdA-fractie vragen hoe wordt voorzien in de mogelijkheid om een nieuwe koppeling te genereren indien er een fout optreedt of als dit wegens veiligheidsredenen nodig is.

Het persoonlijk Dezi-nummer is gekoppeld zo lang de zorgmedewerker in het Dezi-register geregistreerd staat. Indien er grond is om een nieuwe koppeling te genereren, dan is dit op gecontroleerde wijze mogelijk.

6.4 BSN verwerkingsgrondslag bij de zorgaanbieder

De leden van de GroenLinks-PvdA-fractie vragen de regering om meer uitleg te geven over het soort contract dat middelenuitgever en zorgaanbieder met elkaar moeten aangaan, als de uitgifte van middelen niet via de zorgaanbieder verloopt. Wordt er een modelcontract beschikbaar gesteld voor deze afspraken?

Er is niet beoogd dat het Ministerie van VWS een modelcontract opstelt voor de uitgifte van inlogmiddelen die niet via de zorgaanbieder verlopen. Denkbaar is dat koepelorganisaties hun leden op dit punt kunnen ondersteunen.

De leden van de GroenLinks-PvdA-fractie vragen wie erop toeziet dat deze contracten voldoen aan alle eisen en dat zij rechtmatig zijn.

Het certificeringsschema (NSC-7518) van de NEN 7518 wordt gebruikt door certificerende instellingen onder toezicht van de Raad van Accreditatie. Zij controleren of er bewijs is van een contract tussen de zorgaanbieder en de leverancier van inlogmiddelen. In dit schema staan ook de minimale eisen voor het contract tussen de zorgaanbieder en de middelenleverancier.

Zorgaanbieder en middelenleveranciers zijn zelf verantwoordelijk voor het controleren of een dergelijk contract compleet en rechtmatig is.

6.5 Koppeling HR-systeem aan Dezi-register

De leden van de GroenLinks-PvdA-fractie vragen de regering hoe realistisch het is dat HR-systemen automatisch gekoppeld kunnen worden aan het Dezi-register. Zij willen weten of en hoe de regering stimuleert dat HR-systemen hiertoe worden uitgerust.

De regering acht het realistisch en wenselijk dat HR-systemen automatisch kunnen communiceren met het Dezi-register om mutaties, zoals in- en uitdiensttreding of wijziging van bevoegdheden, efficiënt, veilig en foutloos door te geven. Dit vermindert administratieve lasten en draagt bij aan actualiteit en betrouwbaarheid van het register. Het CIBG ontwikkelt een Dezi-HR API gebaseerd op open standaarden (SCIM, REST) die invulling geeft aan het koppelvlak waarmee HR- systemen van zorgaanbieders kunnen communiceren.

De leden van de GroenLinks-PvdA-fractie vragen of het mogelijk is om een Application Programming Interface (API) te ontwikkelen, als een soort standaardcomponent om met het Dezi-register te communiceren, wat makkelijk geïntegreerd kan worden in een HR-systeem?

Het is zeker mogelijk een Application Programming Interface (API) te ontwikkelen die als een standaardcomponent kan dienen om met het Dezi-register te communiceren. Deze API kan eenvoudig worden geïntegreerd in een HR-systeem, omdat de technische koppeling met het Dezi-register wordt gerealiseerd via een veelgebruikte technische standaard, namelijk SCIM (System for Cross-domain Identity Management).

SCIM is een aanbevolen standaard ~~is~~ binnen de Nederlandse overheid. Dit zorgt ervoor dat de techniek breed ondersteund wordt en dat de integratie met verschillende systemen soepel kan verlopen. Veel HR-systemen ondersteunen deze standaard al, waardoor de kans groot is dat een HR-systeem zonder grote aanpassingen kan communiceren met het Dezi-register.

De SCIM-standaard is bovendien goed gedocumenteerd. Dit betekent dat, als een HR-systeem of de leverancier ervan de standaard nog niet ondersteunt, zij gebruik kunnen maken van de uitgebreide documentatie om de benodigde koppeling zelf te ontwikkelen. Dit maakt het eenvoudiger en goedkoper de integratie te realiseren, omdat er geen volledig nieuwe technologie hoeft te worden bedacht. Met deze technische standaard kan de communicatie en het uitwisselen van gegevens tussen het HR-systeem en het Dezi-register efficiënt plaatsvinden. Dit maakt de integratie minder complex en zorgt ervoor dat de gegevens op een gestandaardiseerde manier worden verwerkt.

De leden van de GroenLinks-PvdA-fractie vragen wiens verantwoordelijkheid is het om HR-systemen dusdanig uit te rusten dat de koppeling mogelijk is?

De verantwoordelijkheid voor het daadwerkelijk koppelen van een HR-systeem aan het Dezi-stelsel ligt primair bij de zorgaanbieder en diens softwareleverancier. Het ministerie van VWS stimuleert deze ontwikkeling indirect door het beschikbaar stellen van het standaardkoppelvlak en het ondersteunen van leveranciers met technische ondersteuning en praktijkpilots.

6.6 De koppeling met DUO om diploma's te verifiëren om de jeugd- en zorgmedewerkers te ontlasten

De leden van de GroenLinks-PvdA-fractie begrijpen de koppeling met de Dienst Uitvoering Onderwijs (DUO). Echter vragen zij de regering om zorg te dragen dat er alternatieve methodes blijven bestaan om een diploma, indien nodig, te verifiëren.

Indien de dienstverlening vanuit DUO onverhoopt stil komt te liggen, dan is een alternatieve methode dat de medewerker zelf het diploma kan aanleveren of op een later moment kan gebruikmaken van de dienstverlening van DUO.

De leden van de GroenLinks-PvdA-fractie vragen of een soortgelijke koppeling mogelijk is met niet-Nederlandse diplomaverstrekkers, indien medewerkers hun diploma elders hebben behaald?

Er is geen koppeling mogelijk met niet-Nederlandse diplomaverstrekkers. Indien een zorgverlener is geregistreerd in het BIG-register aan de hand van een buitenlands diploma, dan kan een koppeling worden gemaakt met het BIG-register.

De leden van de VVD-fractie vragen waarom is gekozen voor een vrijblijvend karakter en niet een verplichtend karakter van de koppeling met het diplomaregister van DUO. In hoeverre verhoudt deze vrijblijvende mogelijkheid zich tot de zin «registratie zou alleen mogelijk moeten zijn met een opleiding in de zorg» zoals aangegeven in paragraaf 11.1.7 in de memorie van toelichting?

Het toevoegen van een diploma is niet verplicht opgenomen in het wetsvoorstel, omdat alle zorgmedewerkers zich laagdrempelig moeten kunnen inschrijven voor het gebruiken van een veilig inlogmiddel met betrouwbaarheidsniveau hoog.

Een zorgmedewerker die een beroep uitoefent in de zin van de Wet BIG kan zijn beroepstitel(s) toevoegen aan de registratie. Het Dezi-register voert daarbij een controle uit of de betreffende zorgmedewerker daadwerkelijk deze beroepstitel mag voeren, bijvoorbeeld door een toets bij het BIG-register. Zodra de registratie van een zorgmedewerker is gekoppeld aan een zorgaanbieder, dan kan deze registratie toegang geven tot een zorginformatiesysteem van een zorgaanbieder. Het zorginformatiesysteem moet voldoen aan de NEN 7510, waardoor er op basis van rollen/beroepen toegang gegeven wordt tot medische informatie. Afhankelijk van de rol/beroep, kunnen aanvullende autorisatiekenmerken, zoals een beroepstitel, noodzakelijk zijn om toegang te krijgen tot de juiste informatie.

Er zijn ook functies waar patiëntgegevens worden verwerkt, maar waarvoor geen specifiek diploma vereist zal zijn. Een voorbeeld hiervan zijn medewerkers die administratieve handelingen verrichten. Voor deze medewerkers is het ook belangrijk dat zij een inlogmiddel op betrouwbaarheidsniveau hoog gebruiken.

6.7 De koppeling met het BIG-register om het registratieproces efficiënter en gebruikersvriendelijk te maken voor de jeugd- en zorgmedewerkers

De leden van de GroenLinks-PvdA-fractie vragen de regering om ervoor te zorgen dat de koppeling met het BIG-register altijd een actieve keuze van de medewerker in kwestie blijft, en niet zonder toestemming kruisverbanden te leggen met een mogelijke BIG-registratie bij iedere aanmelding in het Dezi-register.

Aanvullende (autorisatie-)kenmerken, zoals bevoegdheden vanuit de Wet BIG, worden met grote zorgvuldigheid toegekend. Bij de inschrijving in het Dezi-register heeft de medewerker de mogelijkheid diens beroep toe te voegen. Dit kan met de koppeling DUO of met de koppeling met het BIG-register. Het blijft een keuze van de medewerker om diens beroep toe te voegen. De medewerker dient daarvoor dus toestemming te geven. Als er geen beroep wordt toegevoegd, dan kan dit wel tot gevolg hebben dat de autorisatie van de medewerker in het zorginformatiesysteem, niet kloppend is bij zijn functie, waardoor die bijvoorbeeld geen toegang heeft tot (bepaalde) informatie.

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

De leden van de PVV-fractie vragen hoe wordt gegarandeerd dat de nieuwe identificatiemiddelen voldoen aan de strengste normen voor gegevensbescherming.

Alle inlogmiddelen die erkend worden door het wetsvoorstel moeten voldoen aan betrouwbaarheidsniveau hoog. Alleen deze inlogmiddelen mogen worden gebruikt voor het identificeren van personen in de zorg. Dit garandeert namelijk dat de inlogmiddelen voldoende beveiligd zijn tegen fraude en misbruik.

Alleen gekwalificeerde leveranciers van vertrouwensdiensten (*Qualified Trust Service Providers-QTSP's*) mogen inlogmiddelen leveren die voldoen aan het betrouwbaarheidsniveau hoog. Dit betekent dat alleen bedrijven die door de overheid en de Europese Unie zijn goedgekeurd, deze inlogmiddelen mogen leveren. *QTSP's* moeten voldoen aan strikte eisen op het gebied van beveiliging, betrouwbaarheid en gegevensbescherming.

De eisen die gelden voor *QTSP's* zijn ook zeer strikt. Ze moeten voldoen aan de strengste normen voor vertrouwelijkheid en integriteit van gegevens, zoals vastgelegd in de eIDAS-verordening en de AVG. De *QTSP's* worden regelmatig gecontroleerd en geaudit om te zorgen dat ze voldoen aan de hoogste standaarden van gegevensbescherming. Dit zorgt ervoor dat de persoonlijke gegevens van gebruikers goed worden beschermd tegen ongeautoriseerde toegang of verlies.

Artikel 24 van de eIDAS-verordening schrijft verder voor dat *QTSP's* moeten voldoen aan de hoogste normen voor beveiliging en gegevensbescherming. Dit zorgt ervoor dat alle partijen die betrokken zijn bij het leveren van inlogmiddelen, de privacy van gebruikers respecteren en beschermen.

Deze maatregelen garanderen dat de nieuwe inlogmiddelen voldoen aan de strengste normen voor gegevensbescherming en dat de persoonlijke gegevens van gebruikers veilig worden behandeld en in overeenstemming met de wetgeving. Het gebruik van geaccrediteerde QTSP's en de naleving van eIDAS-verordening en de AVG biedt een solide basis voor de bescherming van gevoelige informatie.

De leden van de PVV-fractie vragen of er risico's zijn verbonden aan het gebruik van persoonlijke apparaten voor digitale identificatie, en hoe deze risico's zoveel mogelijk worden vermeden.

Het gebruik van persoonlijke apparaten voor digitale identificatie brengt bepaalde risico's met zich mee. Deze risico's worden gemitigeerd doordat de leverancier van het identificatiemiddel specifieke eisen stelt aan het apparaat waarop het middel wordt gebruikt. Deze eisen kunnen zowel technisch als procedureel van aard zijn. Wanneer het om privé-eigendom van de zorgmedewerker gaat, ligt het beheer van het apparaat – zoals het tijdig uitvoeren van beveiligingsupdates – niet volledig in handen van de zorgaanbieder of de middelenleverancier. Als de zorgmedewerker geen toestemming geeft voor noodzakelijk beheer of het apparaat onvoldoende onderhoudt, kan dit ertoe leiden dat het identificatiemiddel (tijdelijk) niet meer via dat apparaat gebruikt kan worden.

De leden van de GroenLinks-PvdA-fractie vragen de regering om de uitgevoerde data protection impact assessment (DPIA), indien uit veiligheidsoverwegingen noodzakelijk slechts op hoofdlijnen, aan de Kamer te doen toekomen.

Uit veiligheidsoverwegingen kan ik niet de volledige DPIA overleggen. Ik geef daarom hieronder op hoofdlijnen een overzicht van de gesignaleerde risico's en de mitigerende maatregelen.

In de DPIA van het wetsvoorstel is in de eerste plaats het risico gesignaleerd dat het CIBG een groot aantal persoonsgegevens verwerkt, waaruit veel loginformatie is te verkrijgen. Hierop zijn de nodige maatregelen genomen, zoals op het gebied van (*end-to-end-*) versleuteling, het screenen van personeel, de inzet van PET's en dataminimalisatie door het gebruik van data bij de bron.

Daarnaast is het risico van niet-beschikbaarheid van het ontkoppelpunt[35] en het register als risico benoemd. Dit wordt ondervangen door de hoge eisen die zijn gesteld aan de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten. Zo wordt de beschikbaarheid bij een technisch incident snel hersteld en is er een terugvaloptie of noodoplossing beschikbaar. Ook logging,

[35] Het ontkoppelpunt zorgt voor de omzetting van de identiteit van de natuurlijk persoon naar de zorgidentiteit.

monitoring en alerting met bijbehorende 24/7 piketdienst voor het acteren op verstoringen en het opstellen van een bedrijfscontinuïteitsplan in combinatie met het periodiek testen zijn voorbeelden van genomen maatregelen.

Een derde risico werd gezien in het gebruik van het BSN door de zorgaanbieder voor andere doelen. Dit risico wordt ondervangen door controle via audits. Wanneer een zorgaanbieders zorgspecifieke middelen willen uitgeven, dan moeten zij zich namelijk laten certificeren. Hierbij

vindt een audit plaats op het uitgifteproces van een zorgaanbieder. Daarbij wordt gecontroleerd of het BSN juist is verwerkt en dat het na koppeling van identiteiten uit de administratie van de zorgspecifieke middelen is verwijderd. Het ritme van de audits wordt nog door de NEN bepaald.

Tot slot werd de mogelijkheid tot het uitlenen van inlogmiddelen als risico geconstateerd. Gebruikers worden bij het verstrekken van het middel uitgelegd dat het middel niet mag worden gedeeld met derden. Het feit dat dit wetsvoorstel een mogelijkheid creëert om gebruik te maken van verschillende erkende inlogmiddelen verkleint ook het risico dat middelen worden uitgeleend.

Voor Wdo-middelen geldt bovendien dat deze breder gebruikt kunnen worden dan in de zorgsector. Daarmee zal een zorgprofessional minder snel geneigd zijn het middel uit te lenen. Doordat bepaalde middelen voor verschillende doeleinden worden gebruikt, ligt het uitlenen van een mobiele telefoon of ziekenhuispas niet voor de hand. Bijvoorbeeld: een mobiele telefoon wordt minder snel gedeeld, omdat daarop vaak persoonlijk gegevens staan (foto's, WhatsApp-berichten, e-mails en applicaties voor bankieren). Dit maakt het uitlenen minder waarschijnlijk. Het uitlenen van bijvoorbeeld een DigiD-login is niet aantrekkelijk voor de zorgprofessional, omdat op basis van die gegevens misbruik mogelijk is bij onder andere de gemeente, Belastingdienst, of zorgverzekeraar.

De leden van de GroenLinks-PvdA-fractie vragen de regering in overweging te nemen dat het uitwisselen van inlogmiddelen niet moet worden toegestaan, om te voorkomen dat de zorgvuldige veiligheidsmaatregelen en privacy waarborgen (onbedoeld)worden omzeild. Daarmee verliest de wet haar functie. Deze leden vragen of de regering nader kan ingaan op het opnemen in de wet van een bepaling die uitlenen van inlogmiddelen verbiedt, al dan niet het technisch onmogelijk maakt ?

Het is technisch niet mogelijk het uitlenen van een persoonlijk inlogmiddel onmogelijk te maken. Een wettelijk verbod op het uitlenen van inlogmiddelen is niet handhaafbaar. Hierbij benadruk ik dat een zorgaanbieder, in het kader van het treffen van organisatorische maatregelen zoals opgenomen in de AVG, de zorgmedewerker moet wijzen op het feit dat het niet is toegestaan om de inlogmiddelen uit te lenen.

De leden van de GroenLinks-PvdA-fractie vragen welke preventieve maatregelen verder nog kunnen worden genomen om er maximaal voor te zorgen dat inlogmiddelen niet worden uitgeleend of in het geval van diefstal niet te gebruiken zijn?

Indien een middel wordt verloren of is gestolen, dan moet de gebruiker dit direct melden bij de verstrekker van het middel, zodat het middel wordt ingetrokken.

Het principe dat de inlogmiddelen niet uitgeleend mogen worden, kan vergeleken worden met het niet delen en geheim blijven van wachtwoorden. Het systeem is op dit vlak net zo veilig als de mensen die ermee werken. Het informeren van de medewerker over de gebondenheid van het middel aan de persoon en over de te nemen maatregelen bij verlies, of diefstal, is een verantwoordelijkheid van de zorgaanbieder voor wie de medewerker werkt. Deze informatieplicht zal een onderdeel moeten zijn van het pakket aan (organisatorische) beveiligingsmaatregelen dat de zorgaanbieder zelf op grond van de artikel 32 AVG moet nemen.

Indien een middel wordt verloren of is gestolen, dan moet de gebruiker dit daarnaast direct melden bij de verstrekker van het middel zodat het middel kan worden ingetrokken.

Een verbodsbepaling voor het uitlenen van inlogmiddelen zou geen extra waarborg bieden, omdat het toezicht hierop niet uitvoerbaar is. Het uitlenen van inlogmiddelen is niet te controleren door de IGJ noch te voorkomen.

De leden van de GroenLinks-PvdA-fractie hebben bezwaren bij het gebruiken van inlogmiddelen op de privételefoon. Niet alleen is het gezond om personeel in een professionele setting indien mogelijk te voorzien van

een werktelefoon, het biedt ook de noodzakelijke veiligheidswaarborgen. Genoemde leden vragen in overweging te nemen om afspraken over het beheren van privételefoons niet over te laten aan zorgaanbieders en hun personeel. Hierdoor kan namelijk de situatie ontstaan dat medewerkers (impliciete) dwang ervaren om hun privé-telefoon onder beheer van hun werkgever te plaatsen. Erkent de regering dat deze situatie onwenselijk is?

Voor de regering zou het onwenselijk zijn als een situatie ontstaat waarin medewerkers (impliciete) dwang ervaren om hun privé-telefoon onder beheer van hun werkgever te plaatsen. Derhalve wordt met het wetsvoorstel geregeld dat een medewerker de keuze heeft tussen verschillende inlogmiddelen en is dus niet gebonden aan een middel dat is gekoppeld aan een (privé)-telefoon.

Het wetsvoorstel regelt met artikel 15 dat wanneer een voorziening of systeem gebruikt wordt met een goedgekeurd inlogmiddel, de beheerder van deze voorziening of dit systeem de gebruiker in staat moet stellen om ook gebruik te maken van elk ander goedgekeurd inlogmiddel. De mogelijkheid ieder erkend middel te gebruiken biedt zorgmedewerkers die geen gebruik willen maken van een privé-telefoon daarmee alternatieven naast de privé-telefoon om mee in te loggen. Hiermee wordt voorkomen dat de (impliciete) dwang ontstaat de privé-telefoon onder beheer van hun werkgever te plaatsen.

De leden van de GroenLinks-PvdA-fractie vragen hoe wordt voorkomen dat zorgaanbieders hun medewerkers (impliciet) dwingen om hun privételefoon in beheer van de werkgever te plaatsen.

De werkgever is in het kader van zijn zorgplicht van artikel 7:658 BW en goed werkgeverschap in van artikel 7:611 BW verplicht werknemers te voorzien van middelen om hun werkzaamheden te kunnen uitvoeren. De werkgever hoort hierom de werknemer te voorzien van een werktelefoon. De werknemer kan dus niet worden verplicht een privé-telefoon te gebruiken.

Daarnaast maakt dit wetsvoorstel het mogelijk te kiezen tussen verschillende inlogmiddelen. Een werkgever is dus niet gebonden aan een inlogmiddel dat is gekoppeld aan een (privé-)telefoon. Desalniettemin is het onmogelijk om (impliciete) dwang in alle individuele gevallen volledig te voorkomen. Het ligt in de sfeer van de werkgever en de werknemer om afspraken te maken over het gebruik van werk- en of privételefoons, met inachtneming van de geldende arbeidsrechtelijke bepalingen.

De leden van de GroenLinks-PvdA-fractie vragen of de regering van mening is dat dit mogelijk kan leiden tot een inbreuk op de privacy van medewerkers?

Allereerst zij vooropgesteld dat een medewerker op grond van dit wetsvoorstel de keuze heeft tussen verschillende inlogmiddelen en dus niet is gebonden aan een middel dat is gekoppeld aan een telefoon. Bovendien beschermt de eis van goed werkgeverschap van 7:611 BW samen met de zorgplicht van artikel 7:658 BW de medewerker tegen het gedwongen in beheer nemen van zijn privételefoon door de werkgever.

Voor zover de medewerker er zelf voor kiest een middel dat via de mobiele telefoon werkzaam is te gebruiken, dan biedt de bestaande wetgeving voldoende waarborgen om de privacy van deze werknemer te beschermen. Het in beheer nemen van een telefoon (of dat nu een privé- of werktelefoon is) moet immers op grond van de AVG altijd voldoen aan de noodzaak, proportionaliteit en de subsidiariteit, waarbij moet worden getoetst of het belang in verhouding staat tot de inbreuk en of met een minder ingrijpend middel hetzelfde doel kan worden bereikt. Ook moet de medewerker hier vooraf over worden geïnformeerd.

De leden van de GroenLinks-PvdA-fractie vragen of de regering de mogelijkheid ziet om zorgaanbieders een zorgplicht te geven om ervoor te zorgen dat, in het geval er telefonische inlogmiddelen worden gebruikt, de gebruikte (werk)telefoons maximaal beveiligd zijn?

De regering erkent dat de zorgaanbieder een zorgplicht heeft voor de beveiliging van een telefoon waarvan het inlogmiddel gebruik maakt. Deze plicht volgt uit bestaande wet- en regelgeving die een zorgaanbieder verplichten passende technische en organisatorische beveiligingsmaatregelen te nemen. Dit betekent dat de zorgaanbieder moet zorgen dat de telefoons die worden gebruikt bij het inloggen juist moeten zijn beveiligd en dat de medewerkers moet zijn geïnformeerd over de beveiligingsmaatregelen die zij zelf moeten nemen.

De leden van de GroenLinks-PvdA-fractie vragen de regering om in overweging te nemen om het uitlenen van inlogmiddelen en het gebruik van privételefoons per wet te verbieden, of om aanvullende maatregelen te treffen om beide risico's weg te nemen.

Op grond van de zorgplicht van de zorgaanbieder is de regering van mening dat geen aanvullende wettelijke maatregelen vereist zijn.

De leden van de GroenLinks-PvdA-fractie vragen de regering om beide risico's blijvend te monitoren nadat de wet in werking treedt, en zorgaanbieders hierop te wijzen.

Ik onderken het belang van zorgvuldig gebruik van inlogmiddelen en de risico's die zich kunnen voordoen bij bijvoorbeeld het gebruik van privéapparatuur of het uitlenen van middelen. In dat kader blijft het essentieel dat zorgaanbieders hun verantwoordelijkheid nemen om veilige en werkbare oplossingen te faciliteren voor hun medewerkers. De reeds bestaande kaders en normen, waaronder de AVG, de NEN 7510 en NEN7 518, bieden duidelijke handvatten om veilig gebruik te waarborgen.

Er worden bij de implementatie van Dezi zijn indicatoren opgesteld om de voortgang te monitoren zodat tijdig kan worden bijgestuurd. Naast de indicatoren over het aantal aangesloten instellingen en zorgmedewerkers, wordt expliciet aandacht besteed aan de knelpunten zoals ervaren door zorgmedewerkers. De Kamer kan hierover desgewenst jaarlijks via een Kamerbrief over worden geïnformeerd.

De leden van de GroenLinks-PvdA-fractie vragen of de regering ook bereid is om in contact met zorgaanbieders te wijzen op de noodzaak om werktelefoons of alternatieve apparatuur aan medewerkers te bieden die voor hun dagelijkse werk worden geacht om inlogmiddelen te gebruiken.

In de implementatiefase blijft de dialoog met het veld centraal staan, Vanuit een gezamenlijke verantwoordelijkheid wordt toegewerkt naar een zorgvuldige toepassing van het nieuwe stelsel.

De leden van de GroenLinks-PvdA-fractie vragen of de regering bereid is om zorgaanbieders hierin financieel te ondersteunen, indien dit een drempel blijkt.

In de eerste plaats wordt benadrukt dat een medewerker de keuze heeft tussen verschillende inlogmiddelen en dus niet is gebonden aan een inlogmiddel dat is gekoppeld aan een telefoon. Daarnaast is voor zorgaanbieders een stimuleringsregeling voorzien. Hierin draagt de overheid in de eerste twee jaar (2026/2027) bij aan de aanschaf van nieuwe inlogmiddelen. Bij de implementatie zal verder nadrukkelijk aandacht zijn voor de betaalbaarheid, met oog voor sectorale verschillen en schaalgrootte. Het wetsvoorstel biedt in ieder geval de ruimte om de kosten omlaag te brengen door marktwerking en hergebruik van bestaande middelen.

De leden van de NSC-fractie hebben een technische vraag over de beveiliging van het systeem. Hoe wordt veiligheid van inlogmiddelen technisch bewaakt?

De inlogmiddelen moeten zijn uitgegeven door een gekwalificeerde verlener van vertrouwensdiensten. De vertrouwensdienst moet aantoonbaar voldoen aan de eisen vanuit de eIDAS-verordening voor het beveiligen van de systemen beheerd door hen. Deze eisen zijn via uitvoeringshandelingen en normatieve verwijzingen, zoals ETSI-standaarden, verplicht gesteld en vertrouwensdiensten worden periodiek getoetst door een onafhankelijke certificerende instantie op naleving.

Een voorbeeld van een toepasselijke ETSI standaard is *ETSI EN 319 401 General Policy Requirements for Trust Service Providers*, waarin bijvoorbeeld eisen worden gesteld aan de logische en fysieke toegangsbeveiliging van de dienst. Voor gekwalificeerde handtekeningen gelden nog aanvullende eisen, bijvoorbeeld dat de handtekening alleen gekoppeld is aan de ondertekenaar, deze de ondertekenaar kan identificeren en dat de handtekening is gemaakt met behulp van gegevens met een hoge mate van zekerheid.

Er moet gebruik gemaakt worden van certificaten die geproduceerd zijn met gekwalificeerde, hoog beveiligde apparaten, zoals bijvoorbeeld smartcards of *hardware security modules* (*HSM's*). Deze *Qualified Signature Creation Devices* (*QSCD*) moeten op hun beurt ook weer zijn gecertificeerd. Via dit stelsel van eisen, normen en certificeringen wordt de veiligheid van het middel en betrouwbaarheidsniveau hoog geborgd.

De leden van de NSC-fractie hebben een vraag over het bestaan van standaardprotocollen in het geval van complicaties bij gebruik van het nieuwe systeem. Hoe werkt bijvoorbeeld de misbruikdetectie en herstel bij het inloggen in het systeem door een onbevoegd persoon? Zijn er ook standaardprotocollen voor andere typen complicaties?

De inlogmiddelen zijn persoonsgebonden en worden uitgegeven aan zorgmedewerkers op basis van een uitgifteproces op betrouwbaarheidsniveau hoog. Als een zorgmedewerker dit inlogmiddel uitleent of verliest, dan is er risico op het inloggen door een onbevoegd persoon. Dit risico en het risico op verlies van een inlogmiddel kan nooit worden uitgesloten. In zulke situaties is dit niet vast te stellen aan de zijde van het Dezi-register. In het geval de zorgaanbieder dit vaststelt, kan deze de desbetreffende persoon de toegang tot zorgsystemen ontzeggen. De zorgaanbieder moet misbruik ook melden aan de IGJ. Voor infrastructurele inbreuken gelden standaardprotocollen tussen de hosting partij en het Dezi-register.

De leden van de NSC-fractie zijn bezorgd over de gevoeligheid van het nieuwe register voor spionagesoftware en andere malware. Hoe is het Dezi-register beschermd tegen het binnendringen van spionagesoftware zoals Pegasus, Predator of andere malware? Hoe zorgt de regering dat deze bescherming ook in de toekomst up to date blijft?

Het Dezi-register wordt gehost bij een ISO:27001 gecertificeerde provider. Toegang tot de servers wordt gelogd en is beperkt tot specifieke functionarissen. Door inzet van applicatie firewalls, encryptie en zero trust-technieken voorkomen we dat onbevoegden toegang krijgen tot de systemen en data.

Op alle servers is standaard malware scanning software actief. Deze software en zijn configuratie wordt actueel gehouden door actieve configuratie en patch-management. Daarnaast monitort een *Intrusion Detection System* al het inkomende en uitgaande netwerkverkeer. De omgevingen zijn zelf gezoneerd waardoor netwerktechnisch, gelaagde veiligheidszones zorgen voor minimale impact in het geval van compromittering.

De ontwikkelingen op het gebied van beveiliging worden daarnaast nauw gevolgd. Doordat het Dezi-register op een zeer hoog veiligheidsniveau opereert, worden de geïmplementeerde beveiligingstechnieken geüpgraded als er betere beschikbaar komen en deze upgrade opportuun is.

7. Gevolgen (m.u.v. financiële gevolgen)

7.1 Overheid

De leden van de PVV-fractie vragen wie de financiële effecten dragen voor de uitrol van de beoogde effecten van deze wet. Is dit volledig budgettair belast bij het Ministerie van VWS en in welke mate worden zorgorganisaties zelf belast?

De kosten voor de inrichting, ontwikkeling en het beheer van het Dezi-register zijn volledig budgettair gedekt binnen het ministerie van VWS. Dit betreft onder andere: de stelselarchitectuur, de standaardisatie, het centrale koppelvlak, communicatie, begeleiding en ondersteuning bij de implementatie. Zorgaanbieders dragen zelf de kosten voor de aanschaf en inzet van goedgekeurde inlogmiddelen voor hun medewerkers, evenals voor de aansluiting op het Dezi-register. Dit wijkt niet af van de huidige situatie met de UZI-passen.

Er is bewust gekozen voor een open marktmodel, zodat organisaties kunnen kiezen uit meerdere goedgekeurde middelen en zo de kosten kunnen afstemmen op hun situatie. De regering verwacht dat de structurele kosten per gebruiker voor zorgaanbieders lager uitvallen dan bij het huidige UZI-stelsel, mede dankzij concurrentie en schaalvoordelen. Tegelijkertijd worden organisaties ondersteund bij de transitie, met aandacht voor kleinere partijen en sectoren waar de uitvoeringskracht beperkt is.

De leden van de GroenLinks-PvdA-fractie vragen om in een tijdspad uiteen te zetten hoe het CIBG toegroeit / afschaalt naar de gewenste vorm. Deze leden vragen wat het huidige aantal fte is en tot welk aantal zal het CIBG groeien / afschalen?

Voor het uitvoeren van registratiewerkzaamheden en bijbehorende taken voor het UZI-register wordt circa 17 fte ingezet.

Na inwerkingtreding van dit wetsvoorstel zal het registratieproces procesmatig veranderen en komt er daarnaast een proces voor het beoordelen van de authenticatiemiddelen die onderdeel (willen) worden van het stelsel. Er wordt voor het jaar na inwerkingtreding een (tijdelijke) toename verwacht van 4 fte om zowel de werkzaamheden voor het UZI- als het Dezi-register te kunnen uitvoeren. Na een jaar zal de benodigde inzet vervolgens weer afnemen tot de huidige fte van circa 17, doordat de werkzaamheden voor het UZI-register afnemen.

De verdere meerjarige doorkijk op de organisatieontwikkeling, zeker na het uitfaseren van de UZI-pas, laat zich op dit moment nog moeilijk inschatten.

7.2 Zorg- en jeugdveld

De leden van de GroenLinks-PvdA-fractie willen meer weten over de gekozen overstaptermijn tussen de UZI-pas en middelen die gekoppeld zijn aan het nieuwe Dezi-register. Hoe maakt de regering de inschatting dat de overgangsperiode lang genoeg is?

De regering heeft gekozen voor een gefaseerde overgangsperiode tot uiterlijk 1 januari 2029 om zorgaanbieders voldoende tijd en ruimte te geven voor de overstap van het huidige UZI-stelsel naar het nieuwe Dezi-stelsel. Deze termijn is gebaseerd op de omvang en diversiteit van het zorgveld (van ziekenhuizen tot jeugdhulp en eerstelijnszorg), de noodzaak om softwareapplicaties en systemen aan te sluiten op het koppelvlak én de praktijkervaringen uit eerdere digitaliseringstrajecten waaruit blijkt dat een zorgvuldige, stapsgewijze implementatie de slagingskans verhoogt.

De overgangsperiode is ook gekozen om gebruikers van UZI-middelen de geldigheidsduur van de middelen te laten benutten. Een UZI-middel dat tot eind 2025 wordt uitgegeven, heeft een geldigheid van drie jaar; dus tot einde 2028. Daarnaast is het doel van deze periode om zorgaanbieders die UZI-middelen gebruiken een geleidelijke overgang te bieden naar het gebruik van inlogmiddelen die erkend zijn binnen het Dezi-stelsel.

De leden van de GroenLinks-PvdA-fractie vragen waarom er niet is gekozen voor een beperktere overstaptermijn, omdat de noodzaak voor veilige en makkelijke gegevensuitwisseling hoog is?

Hoewel de noodzaak voor veilige en gebruiksvriendelijke gegevensuitwisseling groot is, is het tempo van de overstap afgestemd op uitvoerbaarheid en beschikbaarheid van nieuwe, gecertificeerde inlogmiddelen. De overgangsperiode moet niet alleen technisch, maar ook organisatorisch haalbaar zijn en bovendien geen extra werkdruk leggen op zorgprofessionals.

Zorgaanbieders zijn verantwoordelijk voor de overstap, maar worden hierin ondersteund. Het CIBG en het ministerie van VWS nemen een actieve regierol door: het beschikbaar stellen van een standaard koppelvlak en technische documentatie, het begeleiden van leveranciers via pilots en implementatieondersteuning, het bieden van handreikingen, communicatie en een centrale servicedesk, en het faciliteren van kennisdeling tussen koplopers en andere organisaties.

De leden van de GroenLinks-PvdA-fractie vragen wat de Minister van VWS (of het CIBG) doet in het geval de overstap naar het Dezi-register moeizaam verloopt? Hoe wordt daarin de werkdruk op de zorgaanbieders geminimaliseerd?

Mocht blijken dat de overgang bij bepaalde sectoren of organisaties moeizaam verloopt, dan gaan het ministerie van VWS en het CIBG samen met betrokken partijen tijdig interventies inzetten. Hierbij kan gedacht worden aan gerichte ondersteuning op maat, het onderzoeken van versnelde toelating van inlogmiddelen of andere praktische oplossingen voor een tijdelijke overbrugging.

Het doel blijft altijd om de werkdruk op zorgaanbieders zoveel mogelijk te minimaliseren, terwijl tegelijkertijd de beweging naar een veiliger, toekomstbestendig toegangsmodel onverminderd doorgaat.

De leden van de NSC-fractie willen graag weten hoe dit voorstel het hele zorgveld beïnvloedt. Wat betekent deze wet concreet voor kleine zorgaanbieders?

Het wetsvoorstel heeft gevolgen voor het hele zorgveld: van ziekenhuizen tot eerstelijns zorg, en van wijkverpleging en jeugdhulp tot langdurige zorg. Alle zorgaanbieders die gebruikmaken van elektronische gegevensuitwisseling en die toegang hebben tot cliëntgegevens, moeten zorgdragen voor het gebruik van goedgekeurde inlogmiddelen en aansluiting op het Dezi-register.

Voor kleine zorgaanbieders betekent dit een aantal concrete veranderingen. Zij dienen hun medewerkers te registreren in het Dezi-register, hun systemen (of die van hun leveranciers) aan te sluiten op het koppelvlak van het register en te zorgen voor het gebruik van goedgekeurde inlogmiddelen op betrouwbaarheidsniveau hoog.

De regering is zich ervan bewust dat kleinere aanbieders over minder capaciteit beschikken om nieuwe verplichtingen te implementeren. Daarom wordt tijdens de implementatiefase extra aandacht besteed door sectoraal praktische handreikingen en stapsgewijze begeleiding op te stellen samen met een centrale servicedesk en voorlichtingsmateriaal. Bovendien is gekozen voor een gefaseerde invoering voor UZI-gebruikers tot uiterlijk 1 januari 2029, zodat ook kleinere organisaties voldoende tijd hebben om aan de nieuwe eisen te voldoen.

7.3 Bedrijven

De leden van de PVV-fractie vragen hoe snel zorgaanbieders zich kunnen aanpassen zonder negatieve impact op de patiëntenzorg.

Gezien de variëteit aan zorgaanbieders en de mate waarin en de wijze waarop automatisering geregeld is, is het moeilijk om precies te zeggen hoe snel de overgang naar het Dezi-stelsel kan plaatsvinden. Er is geen eenduidig antwoord, omdat elke zorgaanbieder verschillende stappen zal moeten zetten op basis van hun huidige situatie en automatiseringsniveau. We realiseren ons dat dit voor zorgaanbieders een uitdagende stap kan zijn, en we willen hen hierin zo goed mogelijk ondersteunen.

Om zorgaanbieders te ondersteunen in deze overgang, is er een gefaseerde aanpak voorzien. De huidige UZI-passen en de nieuwe inlogmiddelen uit het Dezi-stelsel gaan een periode naast elkaar bestaan. Dit zorgt ervoor dat zorgaanbieders de tijd hebben om oude middelen geleidelijk te vervangen, terwijl ze tegelijkertijd de patiëntenzorg kunnen blijven ondersteunen met zowel de oude als de nieuwe inlogmiddelen.

Het Dezi-systeem zelf is zo ingericht dat zorgaanbieders maar één technisch koppelvlak hoeven te (laten) realiseren om toegang te krijgen tot alle erkende Dezi-inlogmiddelen. Dit maakt de integratie eenvoudiger, omdat alle middelen via hetzelfde koppelvlak kunnen worden gebruikt.

Zorgmedewerkers kunnen zichzelf op voorhand al registreren in het Dezi-register. Zodra de zorgaanbieder bevestigt dat er een werkrelatie is, kan de zorgmedewerker direct inloggen met een erkend Dezi-inlogmiddel. Dit maakt dat de overstap door de zorgaanbieder wordt bepaald.

Om ervoor te zorgen dat de overgang soepel verloopt, heeft het CIBG een teststraat opgezet voor de relevante technische koppelingen van het Dezi-systeem. Zorgaanbieders en hun leveranciers kunnen deze teststraat gebruiken om alles grondig te testen voordat ze daadwerkelijk de overstap maken. Zodra een zorgaanbieder klaar is met de voorbereiding en het testen, kunnen ze de overstap naar het Dezi-systeem maken. Tot 1 januari 2029 kunnen ze nog steeds de UZI-middelen gebruiken naast de nieuwe Dezi-middelen. Deze aanpak biedt zorgaanbieders voldoende tijd en middelen om zich goed voor te bereiden op de overstap, zodat de overgang naar het Dezi-systeem op een gecontroleerde en efficiënte manier kan plaatsvinden, terwijl de patiëntenzorg doorgaat.

De leden van GroenLinks-PvdA-fractie vragen om een toelichting of en hoe het Ministerie van VWS bedrijven helpt met het maken van de nodige technische aanpassingen in hun systemen.

Er wordt geen standaard softwareoplossing voor integratie in zorgsystemen voorzien. Ontwikkelaars worden wel voorzien van toegankelijke informatie in de vorm van koppelvlakbeschrijvingen en aansluitvoorwaarden zodat aansluiten op het Dezi-register mogelijk wordt. De oplossing maakt gebruik van open standaarden waarmee ontwikkelaars gebruik kunnen maken van standaard componenten. Daarnaast is er ondersteuning beschikbaar in het geval van vragen.

De leden van GroenLinks-PvdA-fractie vragen of de regering bereid is om een open source oplossing te ontwikkelen die bedrijven makkelijk in hun systemen kunnen integreren? Biedt de regering ontwikkelaars handvaten door middel van toegankelijke informatievoorziening over hoe zij kunnen voldoen aan de nieuwe wetgeving?

De bovengenoemde oplossing maakt gebruik van open standaarden zodat ontwikkelaars gebruik kunnen maken van standaard componenten. Bij vragen is er ondersteuning beschikbaar bij het CIBG.

7.4 Burgers

De leden van de PVV-fractie zijn nieuwsgierig welke gevolgen de wetswijziging heeft voor patiënten en cliënten met beperkte digitale vaardigheden.

Er zijn geen gevolgen voor patiënten en cliënten met beperkte digitale vaardigheden. Het stelsel bedient alleen de jeugd- en zorgmedewerkers.

De leden van de GroenLinks-PvdA-fractie zijn van mening dat het wetsvoorstel relatief weinig aandacht heeft voor het belang van burgers. Zij menen dat burgers het volste recht hebben om te weten door wie, wanneer, en met welke reden hun zorggegevens worden geraadpleegd. Kan duidelijker worden toegelicht wat wordt bedoeld met de stelling dat het transparanter wordt wie welke zorggegevens heeft ingezien als identiteiten uit het Dezi-register breed worden gebruikt?

Burgers hebben het recht op inzage in hun medische gegevens en daarmee op transparantie over de verwerking en raadpleging ervan. Dit recht is geregeld via de WGBO, de Wabvpz en de AVG. Op basis van deze wetten kunnen burgers op aanvraag een zogenoemd loggingsoverzicht opvragen bij een zorgaanbieder. Dit wetsvoorstel doet niets af aan de bestaande wetgeving. Bestaande rechten op grond van de WBGO, de Wabvpz en de AVG blijven onverminderd van kracht.

Als onderdeel van de geprioriteerde generieke functies leveren identificatie, authenticatie, autorisatie en logging een belangrijke bijdrage aan veilige en transparante gegevensuitwisseling in de zorg. Door deze functies samen vorm te geven, zoals vastgelegd in het IZA-akkoord, wordt het mogelijk om toegang tot medische gegevens op een controleerbare manier te registreren én te herleiden. Dit ondersteunt burgers bij hun recht op inzage.

Om informatie te geven over wie welke zorggegevens heeft ingezien, is een betrouwbare en eenduidige identificatie van de raadplegende zorgmedewerker noodzakelijk. Zonder deze basis is het voor burgers immers niet inzichtelijk wie hun gegevens heeft ingezien. Het gebruik van identiteiten uit het Dezi-register kan hier aan bijdragen.

De leden van de GroenLinks-PvdA-fractie vragen of burgers proactief worden geïnformeerd als zorgverleners hun gegevens inzien, of kunnen burgers op aanvraag een overzicht ontvangen van hoe hun gegevens zijn opgevraagd en / of verwerkt?

Op dit moment worden burgers in Nederland niet geïnformeerd wanneer een zorgverlener hun gegevens in een medisch dossier bekijkt. Burgers behouden wel hun bovengenoemde recht op inzage.

De leden van de GroenLinks-PvdA-fractie vragen of de regering van mening is dat burgers zelf de baas zijn over hun data, en te allen tijde inzage verdienen in hoe hun gegevens worden verwerkt? Hoe draagt deze wet daaraan bij?

Wat betreft het standpunt dat burgers zelf de baas zijn over hun data. Juridisch eigendom van medische gegevens bestaat niet. Zoals toegelicht in de Kamerbrief over elektronische gegevensuitwisseling van 15 december 2022, zijn persoonsgegevens geen ‘zaken’ en kunnen daarom niet onder het eigendomsrecht vallen.[36]

Dat neemt niet weg dat burgers uitgebreide zeggenschapsrechten hebben. Op basis van de WGBO, de Wabvpz en de AVG beschikken burgers over het recht op inzage, correctie, afscherming en verwijdering van hun medische gegevens. Dit bestaande recht op inzage geldt onverminderd, inclusief de daarbij horende technische en juridische voorwaarden.

De leden van de GroenLinks-PvdA-fractie vragen of de regering mogelijkheden ziet om het recht op inzage voor burgers verder te verstevigen in de wet.

Het wetsvoorstel doet niet af aan de bestaande privacywetgeving over het recht van burgers op inzage in hun medische gegevens. Bestaande rechten op grond van de AVG, de WGBO en de Wabvpz blijven onverminderd van kracht. Tegelijkertijd onderzoekt het ministerie van VWS of de EHDS-verordening voor Nederland aanvullende mogelijkheden biedt om burgers meer regie te geven op hun recht op inzage.

[36] Kamerstukken II 2022/23, 27529 nr. 287.

Verschillende (werk-)groepen in Europa spreken momenteel over de mogelijkheden en wenselijkheid van een proactieve component binnen het inzagerecht. Daarbij spelen overwegingen mee over de technische haalbaarheid, proportionaliteit en impact op werkprocessen in de zorg. Nederland werkt aan de verdere invulling van deze voorstellen en houdt hierbij rekening met uitvoerbaarheid en burgerperspectief. Hierbij wordt afgewogen of het voldoende is om dit te behandelen als onderdeel van de implementatie van de EHDS, of dat een versnelling nodig is om op kortere termijn te voldoen aan nationale wensen rondom proactief informeren.

8. Uitvoering

De leden van de GroenLinks-PvdA-fractie vragen om een nadere uitleg over hoe het CIBG haar taak dient uit te voeren om middelen en inschrijvingen in het UZI-register en het Dezi-register in te trekken of te weigeren. Betekent dit dat het CIBG periodiek de middelen controleert op naleving van de standaarden?

Beleid en uitvoering gaan samen werken aan het stellen van kaders voor de uit te voeren taken op basis van dit wetsvoorstel. Deze nadere kaders worden vastgelegd in onderliggende regelgeving, beleidsregels of andere documentatie. Artikel 14a, tweede lid, onder d, van het wetsvoorstel biedt een grondslag om nadere regels te stellen over de technische inzage in zorgspecifieke middelen. De periodiciteit van de controles op de inlogmiddelen wordt nog vastgesteld.

Zorgspecifieke inlogmiddelen moeten voldoen aan de eisen in NEN 7518. Voor deze inlogmiddelen moet na een audit een conformiteitscertificaat worden overlegd aan het CIBG. Dit certificaat is maximaal 36 maanden geldig. Voor het verstrijken van de geldigheid moet een nieuwe audit plaats vinden. Hiermee wordt gecontroleerd dat zowel het inlogmiddel als de verstrekkende partij voldoen aan de gestelde eisen. Het CIBG controleert of het conformiteitscertificaat is uitgegeven door een conformiteitsbeoordelingsinstantie die gerechtigd is een audit uit te voeren op basis van NEN 7518 en of deze audit op de juiste elementen heeft plaatsgevonden. Daarnaast gaat er een controle plaatsvinden of de leverancier van een inlogmiddel is opgenomen op de Europese vertrouwenslijst van partijen die inlogmiddelen op betrouwbaarheidsniveau hoog uitgeven. Het voornemen is om een overzicht te publiceren van zorgaanbieders die van een zorgspecifieke inlogmiddel gebruik mogen maken.

De leden van de GroenLinks-PvdA-fractie vragen welke methodiek het CIBG hanteert bij het uitvoeren van controles.

Het CIBG controleert of het conformiteitscertificaat is uitgegeven door een conformiteitsbeoordelingsinstantie die gerechtigd is een audit uit te voeren op basis van NEN 7518 en of deze audit op de juiste elementen heeft plaatsgevonden. Daarnaast gaat er een controle plaatsvinden of de leverancier van een inlogmiddel is opgenomen op de Europese vertrouwenslijst van partijen die inlogmiddelen op betrouwbaarheidsniveau hoog uitgeven.

De leden van de GroenLinks-PvdA-fractie vragen of het CIBG technische inzage kan eisen in reeds toegestane middelen ten behoeve van een evaluatie of controle.

De stelselbeheerder krijgt de mogelijkheid om tussentijds te controleren of de middelen nog voldoen aan de vigerende kaders.

De leden van de GroenLinks-PvdA-fractie vragen te onderbouwen dat een besluit in het huidige stelsel onredelijk zwaar kan uitvallen. Om welke besluiten gaat dit, wordt hiermee bedoeld op het intrekken of weigeren van een inlogmiddel? Hoe vaak is dit in het huidige stelsel voorgekomen? Wat kan de regering doen om onvoorziene (hoge) kosten in deze situaties te dempen?

Een voorbeeld van een besluit dat in het huidige stelsel onredelijk zwaar kan uitvallen, is dat bij een doorhaling van een zorgaanbieder in het huidige register alle actieve middelen, zowel de aan de zorgmedewerkers verstrekte UZI-passen als de aan de zorgaanbieder uitgegeven UZI-servercertificaten, worden ingetrokken. De zorgaanbieder kan een (groot) financieel belang hebben bij het tegengaan van de doorhaling en bijbehorende intrekking van de middelen. Bij de afweging tot het doen van een doorhaling en intrekking van de middelen is de continuïteit van de zorg een belangrijk onderdeel.

In het huidige stelsel is een aantal keer sprake geweest van situaties waar doorhaling onredelijk zwaar had kunnen uitvallen, maar waar ik door de toepassing van maatwerk en zorgvuldige afweging van alle belangen gekomen ben tot een evenredige besluitvorming. Bij deze toepassing is op casusniveau beoordeeld hoe tegemoet kon worden gekomen aan het dempen van de kosten voor de zorgaanbieders.

De leden van de GroenLinks-PvdA-fractie vragen of kan worden uitgelegd hoe het bredere gebruik van een middel dan alleen voor de toegang tot de SBV-Z als gevolg kan hebben dat ook andere werkzaamheden worden verstoord. Deze leden vragen of er voorbeelden kunnen worden genoemd van systemen die met gebruik van SBV-Z voor meerdere doeleinden worden gebruikt bij zorgaanbieders?

In de nieuwe situatie wordt een inlogmiddel, naast de toegang tot SBV-Z, ook gebruikt voor toegang tot zorginformatie- en uitwisselingssystemen. Ook kan het worden gebruikt voor het zetten van een gekwalificeerde elektronische handtekening. Een belangrijk uitgangspunt bij dit wetsvoorstel is de keuzevrijheid voor inlogmiddelen. Eén middel moet voor alle soorten systemen gebruikt kunnen worden, zoals bijvoorbeeld inloggen in het patiëntinformatiesysteem en het SBV-Z register.

Afhankelijk van de inrichting aan de zijde van de zorgaanbieder, kan een wijziging van de autorisatiekenmerken er bijvoorbeeld toe leiden dat een zorgverlener (tijdelijk) geen toegang heeft tot het zorginformatiesysteem van de zorgaanbieder.

De leden van de GroenLinks-PvdA-fractie vragen hoe de regering zorgaanbieders stimuleert om niet geheel afhankelijk te worden van slechts één of enkele middelen of aanbieders, om zulke verstoringen in de zorgverlening te voorkomen.

Het is van belang dat zorgaanbieders niet volledig afhankelijk worden van één specifiek inlogmiddel of één aanbieder. In het ontwerp van het Dezi-stelsel is daarom nadrukkelijk gekozen voor een model waarin meer erkende inlogmiddelen kunnen worden gebruikt, mits zij voldoen aan de gestelde eisen. Door zorgaanbieders de mogelijkheid te bieden om te kiezen uit verschillende gecertificeerde middelen en leveranciers, wordt spreiding bevorderd en het risico op verstoringen door afhankelijkheid van één partij beperkt. De interoperabiliteit via een gestandaardiseerd koppelvlak maakt het bovendien mogelijk om binnen één organisatie meerdere middelen naast elkaar te gebruiken, wat de flexibiliteit vergroot.

De leden van de GroenLinks-PvdA-fractie vragen om nader toe te lichten wat zorgaanbieders en individuele zorgmedewerkers in de praktijk gaan merken van het wetsvoorstel. Kan de regering dit beeldend maken?

Voor zorgaanbieders en zorgmedewerkers betekent het wetsvoorstel concreet dat zij veilig en efficiënt kunnen werken met een persoonsgebonden digitaal toegangsmiddel. Zorgmedewerkers moeten zich eenmalig registreren in het Dezi-register. Zorgaanbieders dienen zorg te dragen voor aansluiting van hun systemen op de standaardtechniek.

Voor de zorgmedewerker verandert daarnaast het dagelijkse proces: in plaats van meerdere verschillende inlogmethoden, kunnen zij straks via één gecertificeerd inlogmiddel toegang krijgen tot de benodigde systemen en gegevens. Functiewijzigingen of een wisseling van werkgever vereisen daarbij geen nieuw middel; de registratie in het Dezi-register wordt actueel gehouden, zodat de toegang dynamisch wordt aangepast aan de actuele bevoegdheden van de medewerker. Er is een website beschikbaar met een demonstratie van het ophalen van de zorgidentiteit in de praktijk.[37]

De leden van de NSC-fractie vragen of het Dezi-register technisch robuust genoeg is voor een landelijke schaal mochten alle 1,5 miljoen zorgverleners gebruik gaan maken van dit systeem.

Het Dezi-register is ontworpen als een schaalbare oplossing met als doel om deze beoogde belasting aan te kunnen. Hierbij wordt gebruik gemaakt van bewezen schaalbare technologieën.

9. Regeldruk

9.1 Werkbare invoering in de praktijk

De leden van de PVV-fractie willen graag weten in hoeverre deze wetswijziging zorgt voor een verhoging van administratieve lasten voor zorginstellingen?

[37] Open Demo Lab, *Demonstratie De Zorgidentiteit*.

De regering verwacht dat de invoering van het Dezi-stelsel op de korte termijn een administratieve inspanning vraagt van zorginstellingen, met name rond aansluiting op het Dezi-stelsel en het selecteren van nieuwe inlogmiddelen. Zodra dit echter gebeurd is, leidt het stelsel tot structurele verlaging van administratieve lasten, doordat het beheer van inlogmiddelen gestandaardiseerd, persoonsgebonden en centraal beheerd wordt. Dit voorkomt (zeer bewerkelijk) herhaald uitgiftebeheer, dubbele registraties en onveilige noodoplossingen.

De leden van de PVV-fractie vragen of er voldoende middelen en ondersteuning beschikbaar zijn om zorgorganisaties en zorgverleners te helpen met de overgang naar de nieuwe digitale identificatiemiddelen. Deze leden vragen ook hoe wordt omgegaan met situaties waarin zorgaanbieders of jeugdhulpverleners nog niet klaar zijn om de nieuwe digitale identificatie verplicht te implementeren.

Om zorgorganisaties en zorgverleners te ondersteunen, wordt vanuit het ministerie van VWS en het CIBG ingezet op praktische ondersteuning, communicatie, handreikingen, een 'eenvoudig' koppelvlak en praktijkpilots. Hierbij is ook aandacht voor kleinere zorgaanbieders en sectoren met beperkte uitvoeringscapaciteit.

Het wetsvoorstel voorziet bovendien in een gefaseerde invoering tot uiterlijk 1 januari 2029. Gedurende deze overgangsperiode kunnen bestaande UZI-middelen nog worden gebruikt. Wanneer een zorgaanbieder of jeugdhulpverlener tijdelijk nog niet klaar is om volledig over te stappen, dan biedt deze overgangstermijn ruimte voor stapsgewijze implementatie. De regering acht het stelsel daarmee uitvoerbaar, proportioneel en werkbaar voor het gehele zorgveld.

De leden van de GroenLinks-PvdA-fractie lezen dat enkele zorgaanbieders en zorgketens naar verwachting snel zullen overgaan op de nieuwe inlogmiddelen. Kan de regering haar verwachting voor snelle implementatie van de nieuwe inlogmiddelen uiteenzetten in de tijd? Deze leden vragen ook welk aandeel van zorgaanbieders per 1 januari 2027 en per 1 januari 2028 overgestapt moet zijn voor de sector als geheel om op schema te liggen?

De regering verwacht dat enkele grote zorgaanbieders en zorgketens relatief snel zullen overgaan op het gebruik van de nieuwe inlogmiddelen. Tegelijkertijd moet worden onderkend dat de implementatie en adoptie van het Dezi-stelsel niet exact in concrete percentages of tijdspaden te voorspellen is. De snelheid waarmee zorgaanbieders aansluiten, is mede afhankelijk van sectorale verschillen, leveranciersontwikkelingen en interne prioriteiten binnen organisaties. De genoemde inschattingen voor 2027 en 2028 zijn indicatief en bedoeld om richting te geven aan de gewenste voortgang, maar blijven onder voorbehoud van ontwikkelingen in het zorgveld.

De leden van de GroenLinks-PvdA-fractie vragen hoe implementatie per keten binnen de zorgsector zal verschillen. Zijn er bepaalde ketens in het zorgveld waarvan verwacht wordt dat implementatie relatief moeizamer verloopt en meer tijd kost?

Tijdens de implementatiefase blijft het ministerie van VWS actief in gesprek met het zorgveld. Dit gebeurt via structureel overleg met koepelorganisaties, branchepartijen, leveranciers en zorgaanbieders uit verschillende sectoren. In deze overleggen worden knelpunten, voortgang en ondersteuningsbehoeften besproken. Signalen die daaruit voortkomen worden gebruikt om waar mogelijk gerichte ondersteuning te bieden, zoals praktijkpilots en aanvullende handreikingen.

In de implementatieaanpak wordt nadrukkelijk rekening gehouden met sectorale verschillen. Grote instellingen, zoals ziekenhuizen en GGZ-instellingen, beschikken doorgaans over de middelen en infrastructuur om sneller te kunnen aansluiten. In sectoren zoals de langdurige zorg, jeugdhulp en kleinere eerstelijnsorganisaties zal implementatie naar verwachting meer tijd vergen.

De leden van de GroenLinks-PvdA-fractie vragen wat de regering doet om aanbieders waarbij de overstap naar verwachting meer tijd kost specifiek te ondersteunen om ook over te stappen?

Om zorgorganisaties en zorgverleners te ondersteunen, wordt vanuit het ministerie van VWS en het CIBG ingezet op praktische ondersteuning, communicatie, handreikingen, 'eenvoudig' koppelvlak en praktijkpilots. Hierbij is ook aandacht voor kleinere zorgaanbieders en sectoren met beperkte uitvoeringscapaciteit.

Het wetsvoorstel voorziet bovendien in een gefaseerde invoering tot uiterlijk 1 januari 2029. Gedurende deze overgangsperiode kunnen bestaande UZI-middelen nog worden gebruikt. Wanneer een zorgaanbieder of jeugdhulpverlener tijdelijk nog niet klaar is om volledig over te stappen, biedt deze overgangstermijn ruimte voor stapsgewijze implementatie. De regering acht het stelsel daarmee uitvoerbaar, proportioneel en werkbaar voor het gehele zorgveld.

De leden van de GroenLinks-PvdA-fractie dringen aan op een goede implementatie van deze wet. Hoe blijft de regering in gesprek met het zorgveld om de succesvolle implementatie te monitoren en waar nodig (gericht) hulp te bieden?

Het CIBG speelt als beheerder van het register hierin een uitvoerende rol, onder meer via een servicedesk, communicatiekanalen en begeleiding van sectoren die meer ondersteuning nodig hebben. Op die manier wordt de voortgang gevolgd en kan tijdig worden bijgestuurd, zonder onnodige regeldruk te veroorzaken.

De leden van de GroenLinks-PvdA-fractie vragen hoe de regering ervoor zorgt dat de implementatie samenhangt met andere relevante wetgeving, zoals de Wet elektronische gegevensuitwisseling in de zorg (hierna: Wegiz)?

Er wordt nauw samengewerkt met de uitvoeringsprogramma's van andere relevante wetgeving, zoals de Wegiz. De implementaties van Dezi en Wegiz worden in samenhang afgestemd, zodat eisen rond digitale toegang en gegevensuitwisseling elkaar versterken in plaats van overlappen. Het uitgangspunt is één samenhangende infrastructuur die veilig, herbruikbaar en toekomstbestendig is, waarbij ook de administratieve lasten voor zorgaanbieders zoveel mogelijk worden beperkt.

De leden van de GroenLinks-PvdA-fractie benadrukken het belang om ook Caribisch Nederland te betrekken in het wetsvoorstel. Hoe gaat deze wet vorm krijgen in heel het Koninkrijk? Wat is het tijdspad voor implementatie op de BES-eilanden en de CAS-eilanden?

Ten aanzien van de positie van Caribisch Nederland (de BES-eilanden) merkt de regering op dat hierover gesprekken zijn gevoerd met vertegenwoordigers van de BES-eilanden. De digitale infrastructuur in Caribisch Nederland is echter nog in beperkte mate ontwikkeld, maar inmiddels zijn meerdere digitaliseringstrajecten in de zorgsector gestart. Daarom is er in de implementatie voor gekozen om voor de BES-eilanden te verkennen wat het Dezi-stelsel zou kunnen betekenen.

De regering blijft in gesprek met de bestuursorganen van de BES-eilanden om te bezien hoe en wanneer aansluiting mogelijk en wenselijk is. Voor de CAS-landen (Curaçao, Aruba en Sint Maarten) geldt dat zij zelfstandig verantwoordelijk zijn voor hun eigen zorg- en digitaliseringsbeleid. Dit wetsvoorstel strekt zich daarom niet tot hen uit.

De leden van de NSC-fractie vragen hoe werkbaar het nieuwe register is voor kleine praktijken en zzp'ers en hoe realistisch is het scenario dat zijde verbetering in interoperabiliteit door dit nieuwe register ook daadwerkelijk kunnen benutten?

De regering is zich ervan bewust dat kleinere zorginstellingen en zzp'ers minder capaciteit hebben om nieuwe verplichtingen en digitaliseringsopgaven te implementeren dan grotere instellingen. Juist daarom wordt bij de inrichting van het Dezi-stelsel nadrukkelijk rekening gehouden met de werkbaarheid voor deze groepen.

Het Dezi-register en de toegelaten inlogmiddelen zijn namelijk ontworpen met het uitgangspunt dat aansluiting laagdrempelig moet zijn, ongeacht de omvang van de organisatie. Door het beschikbaar stellen van een standaardkoppelvlak en het mogelijk maken van aansluiting via bestaande leveranciers of collectieve diensten, wordt de administratieve en technische last voor kleine praktijken en zzp'ers zoveel mogelijk beperkt.

Daarnaast biedt het open karakter van het stelsel keuzevrijheid in erkende middelen, waardoor kleine aanbieders kunnen kiezen voor een oplossing die past bij hun schaalgrootte en werkpraktijk, zoals mobiele applicaties of persoonlijke digitale sleutels.

De interoperabiliteit die met het Dezi-register wordt gerealiseerd, is ook voor kleinere zorgaanbieders relevant. Juist doordat zij vaak samenwerken in netwerken of ketens (zoals eerstelijnszorg, wijkverpleging of jeugdteams) profiteren zij van een uniforme, veilige toegangsmethode. Daarmee wordt het eenvoudiger om over de instellingsgrens veilig gegevens uit te wisselen.

9.2 Inloggen met Wdo middelen

De leden van de GroenLinks-PvdA-fractie steunen de kostenverlaging als gevolg van deze wet. Zij erkennen dat het aanvragen van een UZI-pas duur is en verwelkomen goedkopere en gebruiksvriendelijke alternatieven. Hoe faciliteert en stimuleert de regering Nederlandse ondernemers om concurrerende inlogmiddelen te ontwikkelen?

De regering onderschrijft het belang van goedkopere en gebruiksvriendelijkere alternatieven voor de huidige UZI-passen, waarvan de kosten relatief hoog zijn. Een belangrijk doel van het Dezi-stelsel is dan ook om marktwerking mogelijk te maken, zodat meerdere aanbieders concurrerende, veilige en toegankelijke inlogmiddelen kunnen ontwikkelen. Door het open karakter van het stelsel en de standaardisatie van koppelvlakken en certificeringseisen wordt ruimte geboden aan innovatieve Nederlandse en Europese ondernemers.

De regering faciliteert deze marktontwikkeling door transparantie te bieden over de gestelde eisen, tijdige communicatie over de uitfasering van UZI-middelen (met een harde deadline op 1 januari 2029), en door het toegankelijk maken van technische documentatie voor aansluiting op het Dezi-register. Er wordt actief samengewerkt met koepelorganisaties, leveranciers en brancheverenigingen om innovatie en toetreding van nieuwe partijen te stimuleren.

De leden van de GroenLinks-PvdA-fractie vragen wat een acceptabele prijs is voor de te ontwikkelen inlogmiddelen?

Een concrete prijsnorm voor nieuwe inlogmiddelen wordt niet door de regering vastgesteld. Een aanzienlijke verlaging ten opzichte van de huidige kosten van UZI-passen (€255 per pas, exclusief administratiekosten) wordt als wenselijk en realistisch beschouwd. Door marktwerking en schaalvoordelen wordt verwacht dat structureel goedkopere oplossingen ontstaan, ook voor kleinere zorgaanbieders.

De leden van de GroenLinks-PvdA-fractie vragen welke rol de Minister van VWS, of collega-bewindspersoon van Economische Zaken, heeft om het Nederlandse ICT-veld en het zorgveld dichter bij elkaar te brengen om kwalitatieve inlogmiddelen te ontwikkelen?

Ik heb de regierol in het stimuleren van deze marktontwikkeling binnen het zorgdomein. De Minister van Economische Zaken en Klimaat is niet direct betrokken bij dit traject. Het ministerie van VWS onderhoudt regelmatig contact met (koepel)organisaties van zorg-ICT-leveranciers.

De leden van de GroenLinks-PvdA-fractie vragen hoe de regering voorkomt dat er marktdominantie plaats zal vinden van slechts één of enkele partijen?

Om marktdominantie te voorkomen wordt ingezet op een open toelatingsregime. Hierbij kunnen meerdere gecertificeerde middelen via het Dezi-koppelvlak worden gebruikt. De technische en organisatorische inrichting voorkomt *vendor lock-in*, zodat zorgorganisaties flexibel kunnen blijven in hun keuze van middelen en aanbieders.

De leden van de GroenLinks-PvdA-fractie vragen om de verdeling van de financiële lasten nader toe te lichten. Voor wiens rekening zijn de verwachte kosten van inlogmiddelen en de bijdrage aan het Dezi-register? Hoe zorgt de regering ervoor dat medewerkers zelf hier maximaal in worden ontzien?

Wat betreft de financiële lasten geldt dat de kosten voor inlogmiddelen en de aansluiting op het Dezi-register primair de verantwoordelijkheid zijn van de zorgaanbieders.

9.3 Inloggen met zorgspecifieke middelen

De leden van de GroenLinks-PvdA-fractie vragen om toe te lichten hoe zorgaanbieders die zorgspecifieke middelen willen laten goedkeuren worden ondersteund. Zij benadrukken dat het begrijpelijk moet zijn hoe aan standaarden voldaan kan worden en welke informatie moet worden aangeleverd om gecertificeerd te worden.

De regering heeft NEN de opdracht gegeven een norm te ontwikkelen die zorgaanbieders helpt te voldoen aan de eisen voor het onder hun verantwoordelijkheid uitgeven van zorgspecifieke inlogmiddelen. Deze norm is uiteindelijk vastgelegd in NEN 7518 en richt zich op zorgaanbieders. Daarnaast is er een toetsingskader ontwikkeld voor certificerende instellingen: het NSC7518. Dit toetsingskader beschrijft welke informatie zorgaanbieders moeten aanleveren om gecertificeerd te worden volgens NEN 7518. Het doel van dit toetsingskader is ervoor te zorgen dat zorgaanbieders voldoen aan de gestelde eisen, zodat zij

op een veilige en betrouwbare manier kunnen werken met zorgspecifieke inlogmiddelen. Door de norm en het toetsingskader te bekijken wordt duidelijk hoe aan standaarden voldaan kan worden en welke informatie moet worden aangeleverd om gecertificeerd te worden.

NEN 7518 is samen met het veld opgesteld, wat betekent dat er brede input is verzameld van verschillende belanghebbenden in de zorgsector. Deelname aan de werkgroep was open voor iedereen. Hiernaast was de norm tot eind juni 2025 beschikbaar voor publieke consultatie. De verwerking van de reacties op de publieke consultatie is sinds de sluiting van de publieke consultatie op 24 juni 2025 onderhanden bij NEN en zal naar verwachting na de zomer van 2025 een geactualiseerde versie van de norm opleveren.

9.4 De identiteit van een medewerker in het Dezi-register

De leden van de GroenLinks-PvdA-fractie vragen de regering om het gigantische verschil tussen UZI-registraties (90.000) en het potentiële aantal Dezi-registraties (1.500.000) te duiden. Waarop is de aanname gebaseerd dat er elk jaar zo'n 100.000 nieuwe registraties bij zullen komen?

Het verwachte verschil tussen het huidige aantal actieve UZI-registraties (ca. 90.000) en het potentiële aantal Dezi-registraties (ca. 1,5 miljoen) komt doordat het nieuwe stelsel een ander karakter heeft. Ten eerste, is het UZI-stelsel beperkt tot de zorg. De jeugdzorg is hier niet op aangesloten. Ten tweede is het UZI-stelsel beperkt tot een selecte groep medisch beroepsbeoefenaren, namelijk alleen BIG-geregistreerden, die werken met het BSN binnen SBV-Z. Daarentegen is het Dezi-register voor álle zorg- en jeugdhulpmedewerkers die in hun functie toegang nodig hebben tot cliëntgegevens. Dit betreft ook administratief personeel, jeugdhulpprofessionals, wijkverpleegkundigen en andere functionarissen die nu buiten het UZI-stelsel vallen, maar die wel werken met medische gegevens.

De raming van circa 100.000 nieuwe registraties per jaar is gebaseerd op de inschatting dat in totaal ongeveer 1,5 miljoen zorg- en jeugdhulpprofessionals in aanmerking komen voor registratie in het Dezi-register.

De leden van de GroenLinks-PvdA-fractie vragen welke andere dan de in de toelichting genoemde groeiscenario's de regering heeft uitgedacht? Kunnen deze berekeningen worden gedeeld? Wordt er rekening gehouden met het waarschijnlijke groeiaantal in de financiële gevolgen van de wet?

Voor de financiële en uitvoeringsraming is gekozen voor een eerste scenario met een gelijkmatige jaarlijkse groei, oplopend naar het totaal van 1,5 miljoen geregistreerden richting het jaar 2031. Daarbij is aangenomen dat de instroom in de beginjaren gemiddeld circa 100.000 registraties per jaar gaat bedragen. Naar verwachting zal dit aantal in het tweede jaar toenemen, naarmate meer organisaties voorbereid zijn en de implementatie op gang komt.

Tegelijkertijd wordt erkend dat de realiteit anders kan verlopen. De daadwerkelijke groei kan schoksgewijs zijn of juist langzamer verlopen in sommige sectoren. Daarom zijn er alternatieve scenario's doorgerekend, waarbij rekening is gehouden met verschillen in adoptiesnelheid per sector. In sommige scenario's sluiten grotere instellingen eerder aan, terwijl in andere scenario's er juist vertraging optreedt bij kleinere of minder digitaal volwassen zorgaanbieders.

Er is bij het opstellen van de financiële paragraaf en de begrotingsvoorbereiding rekening gehouden met de verwachte groei van het aantal registraties.

10. Financiële gevolgen

10.1 Eenmalige kosten

De leden van de GroenLinks-PvdA-fractie vragen toe te lichten hoe de bouw aan het nieuwe stelsel en uitfasering van het oude stelsel binnen het Ministerie van VWS worden belegd. Wordt hierin gebruik gemaakt van interne expertise?

De bouw van het nieuwe stelsel en de uitfasering van het UZI-stelsel gebeurt binnen het ministerie van VWS door een multidisciplinair programmateam bij het CIBG, dat optreedt als beheerder van het Dezi-stelsel. Deze team bestaan uit interne en externe medewerkers. Door de gekozen opbouw van de team is er borging van de benodigde kennis binnen de huidige organisatie.

Binnen VWS wordt gebruikgemaakt van zowel interne beleids- en ICT-expertise en, waar nodig, van externe specialistische kennis, bijvoorbeeld voor productontwikkeling.

De leden van de GroenLinks-PvdA-fractie vragen toe te lichten op basis van welke indicatoren de regering tot de raming van 14 miljoen euro komt.

De raming van de kosten (19 miljoen euro) is tot stand gekomen op basis van een combinatie van historische kosten uit het huidige UZI-stelsel, verwachte schaalgroei in het aantal gebruikers, geraamde kosten voor beheer en ontwikkeling van het register, en inschattingen van kosten voor certificering, ondersteuning en communicatie. De raming wordt periodiek herijkt op basis van voortschrijdend inzicht en voortgang.

De leden van de GroenLinks-PvdA-fractie vragen of het ICT-team ter beschikking van het Ministerie van VWS voor de Proof of Concept/PoC's en pilots ook volledig uit intern personeel bestaat. Deze leden vragen ook hoe de regering ervoor zorgt dat het ICT-gerelateerde werk zo veel mogelijk intern belegd wordt zodat kennis binnenshuis wordt opgebouwd en behouden.

Het ICT-team verantwoordelijk voor het begeleiden van Proof of Concepts en pilots bestaat deels uit intern personeel en deels uit tijdelijke externe ondersteuning. Waar mogelijk wordt de inhoudelijke aansturing, architectuur en beleidskoppeling door interne medewerkers gedaan, om kennisopbouw binnen VWS te borgen. Er wordt bewust naar gestreefd om zoveel mogelijk ICT-gerelateerd werk intern te beleggen of binnen rijksdiensten te organiseren, zodat ervaring, kennis en continuïteit op lange termijn behouden blijven. De inzet is erop gericht om met een stabiel en lerend team het stelsel duurzaam en beheersbaar op te bouwen, met een blijvende plek voor kennis in de rijksdienst.

10.2 Structurele kosten

De leden van de PVV-fractie vragen welke extra financiële lasten de wetswijziging met zich meebrengt voor zorgaanbieders, en hoe realistisch het is dat deze kosten worden gecompenseerd.

De invoering van het Dezi-stelsel brengt extra financiële lasten met zich mee voor zorgaanbieders. Dit betreft vooral de kosten voor aansluiting op het Dezi-register en de aanschaf of inzet van erkende inlogmiddelen voor medewerkers. Naar verwachting zullen de kosten per gebruiker echter lager uitvallen dan bij gebruik van de huidige UZI-middelen doordat er meer keuzevrijheid, marktwerking en schaalvoordelen zijn.

Het ministerie van VWS is voornemens het gebruik van goedgekeurde inlogmiddelen te stimuleren, maar financiert de gebruikskosten van deze inlogmiddelen niet structureel. De kosten voor veilige toegang worden beschouwd als onderdeel van de reguliere bedrijfsvoering van zorgaanbieders. Om de implementatie beheersbaar te maken, wordt ondersteuning geboden in de vorm van standaardkoppelvlakken, praktische hulpmiddelen en voorlichting. Ook helpt de duale periode tot uiterlijk 1 januari 2029 met het huidige UZI-register om voor deze gebruikers de kosten over meerdere jaren te spreiden.

De leden van de PVV-fractie vragen hoe de continuïteit van digitale toegang wordt gewaarborgd bij technische of financiële belemmeringen, denk daarbij aan storingen of digitale aanvallen van buitenaf die steeds meer toenemen?

Voor de continuïteit van digitale toegang zijn hoge eisen gesteld aan de betrouwbaarheid, beschikbaarheid en beveiliging van het Dezi-stelsel. Gecertificeerde inlogmiddelen op betrouwbaarheidsniveau hoog zorgen voor een veilige toegang. De onderliggende infrastructuur van het register is daarnaast dubbel uitgevoerd en beveiligd volgens rijksnormen. Bovendien worden procedures ingericht voor incidentmanagement, noodtoegang en snel herstel bij storingen. Tevens worden penetratietesten en scans op kwetsbaarheden uitgevoerd. Dankzij deze maatregelen wordt een veilige en betrouwbare toegang tot cliëntgegevens geborgd, ook bij toenemende digitale dreigingen.

De leden van de PVV-fractie constateren dat er landelijk geld wordt geïnvesteerd in digitalisering in de richting van het delen van clientgegevens, maar ook dat er regionaal financiële middelen beschikbaar worden gesteld voor zorgorganisaties om hiermee aan de slag te gaan. Kan de regering aangeven wat hierin de visie is, waarbij

een regionale zorgorganisatie ervoor kan kiezen met een methode te werken die niet in staat is om te delen met de gekozen landelijke methode?

De IZA-transformatiemiddelen worden ingezet om regionale samenwerkingen te financieren die leiden tot het toegankelijk, kwalitatief goed en betaalbaar houden van de zorg, met de focus verschuivend van ziekte naar gezondheid. Het delen van gegevens kan een onderdeel zijn van deze transformatieplannen. Via leidraden toetsen de beoordelende zorgverzekeraars of de regionale plannen aansluiten bij de landelijke ontwikkelingen op gegevensuitwisseling en databeschikbaarheid. Hierbij wordt er dus aan de voorkant op gestuurd dat de ontwikkelingen aansluiten op het landelijke beleid.

De leden van de PVV-fractie vragen of het niet een prioriteit zou moeten zijn om er aan de voorkant voor te zorgen dat de implementatiemethode aansluitend is aan het geheel? Deze leden zien belemmeringen omdat door deze twee aparte financiële stromingen het geheel moeilijker tot stand zal komen.

Het kan voorkomen dat tijdelijke oplossingen worden gefinancierd als de landelijke oplossing nog niet beschikbaar is en ook niet op korte termijn beschikbaar komt. Deze tijdelijke oplossingen moeten door de zorgaanbieders op termijn wel om te zetten zijn naar de structurele landelijke oplossing.

De leden van de GroenLinks-PvdA-fractie vragen de inschatting van 6 miljoen euro als structurele beheerkosten te onderbouwen. Op basis van welke indicatoren is tot deze inschatting gekomen?

De inschatting van 6 miljoen euro is gebaseerd op de huidige inzet van circa 17 fte voor het UZI-register. De inzet hiervan blijft naar verwachting gelijk voor het Dezi-register. Daarnaast zijn hierin de kosten meegenomen van ICT-componenten, zoals applicatie en hosting, om het voeren en instandhouding van een register mogelijk te maken.

De leden van de GroenLinks-PvdA-fractie vragen uit hoeveel fte het team bestaat van VWS-medewerkers dat het stelsel beheert en of hier maximaal ingezet wordt op interne krachten.

Het beheren van het Dezi-stelsel is een nieuwe taak voor het CIBG. Om invulling te geven aan de rollen, bijvoorbeeld stelsel- of ketenbeheerder, om het stelsel te beheren is er 4 fte extra voorzien aan CIBG zijde. Bij voorkeur wordt dit ingevuld met interne krachten.

De leden van de GroenLinks-PvdA-fractie vragen om de prijs van 11 cent per DigiD-inlog te duiden.

De prijs van circa 11 cent per DigiD-inlog betreft de gemiddelde kostprijs die Logius, de beheerder van DigiD, berekent voor een individuele authenticatiehandeling. Dit bedrag dekt de kosten voor beheer, beveiliging, infrastructuur, onderhoud en doorontwikkeling van DigiD. De kostprijs is gebaseerd op het huidige gebruiksniveau, waarbij DigiD miljoenen keren per jaar wordt ingezet, en schaalvoordelen die zorgen voor een relatief lage prijs per inlog. Deze prijs kan in de toekomst nog fluctueren, afhankelijk van gebruiksvolumes en aanvullende beveiligingseisen door bijvoorbeeld nieuwe regelgeving.

De leden van de VVD-fractie vragen wanneer er duidelijkheid wordt verwacht over de financiering voor (aankomende) private middelen onder de Wdo.

Ik verwacht in de loop van 2025 duidelijkheid te krijgen over de financiering van additionele private middelen onder de Wet digitale overheid.

De leden van de VVD-fractie vragen op welke wijze rekening wordt gehouden in de begroting met onzekerheden over gebruikskosten en het beschikbaar komen van digitale wallets in de zorg.

De verwachting is dat de EU Digital Identity Wallet in november 2026 beschikbaar is in Nederland. Het ministerie van VWS is voornemens het gebruik van goedgekeurde inlogmiddelen te stimuleren, maar financiert de gebruikskosten hiervan niet structureel. De kosten voor het gebruik van goedgekeurde inlogmiddelen worden gedragen door zorgaanbieders.

De onzekerheden rond marktontwikkeling en snelheid van adoptie zijn bekend, maar er zijn geen reserveringen in de begroting opgenomen om de structurele gebruikskosten van deze middelen voor zorgaanbieders te dekken. De verantwoordelijkheid voor kostenbeheersing en de keuze van inlogmiddelen ligt bij de aanbieders en zorginstellingen zelf, binnen het wettelijk vastgestelde kader.

De leden van de VVD-fractie vragen wat het verschil is tussen de lagere kosten per gebruiker en de stijging van structurele kosten door de overstap naar Dezi.

Hoewel de structurele kosten in het nieuwe stelsel naar verwachting zullen toenemen, is dit vooral het gevolg van een sterke toename van het aantal geregistreerde gebruikers ten opzichte van de huidige situatie met UZI-middelen. Deze stijging is niet het resultaat van hogere kosten per gebruiker. De kosten per inlogmiddel zullen naar verwachting juist aanmerkelijk lager uitvallen dan bij de huidige UZI-middelen.

De leden van de CDA-fractie lezen dat de kosten voor authenticatie kunnen afhangen van de geldigheidsduur van een zorgidentiteit (bijvoorbeeld een dag of een week). Deze leden vragen of zij goed begrijpen dat dit wetsvoorstel niet voorziet in regels met betrekking tot de geldigheidsduur van een identificatie in relatie tot de kosten. Genoemde leden vragen of dit klopt, en waarom dit wel of niet aan de orde is.

Er is een delegatiegrondslag voorzien voor het stellen van nadere regels over de duur van de identificatie. De jaarlijkse vergoeding gaat een vast bedrag betreffen, dat onafhankelijk zal zijn van het gebruik van het inlogmiddel en/of de geldigheidsduur ervan. Hiervoor is gekozen, omdat differentiatie te veel uitvoeringslasten met zich mee zou brengen.

11. Advies en consultatie

11.1 Internetconsultatie

11.1.1 Scope wetsvoorstel

De leden van de GroenLinks-PvdA-fractie herkennen de onduidelijkheid over de scope van het wetsvoorstel. Zij lezen dat het gebruiken van authenticatie voor interne raadpleging van informatie bijna als toevalligheid een voordeel is geworden van deze wet. Volgens genoemde leden is het gepast om expliciet te maken dat het gebruiken van een veilige methode voor identificatie en authenticatie een doel is van de wet, om zo het uniforme gebruik van de nieuwe inlogmiddelen breed te stimuleren.

In navolging van het advies van de Afdeling advisering van Raad van State is in artikel 15 van het wetsvoorstel een verplichting opgenomen om de goedgekeurde inlogmiddelen te gebruiken voor de toegang tot elektronische uitwisselingssystemen en zorginformatiesystemen. Dit betreft de interne raadpleging. Het belang en de noodzaak daartoe is uitgewerkt in de memorie van toelichting onder paragraaf 2.3.

11.1.2Verplichting wetsvoorstel

De leden van de GroenLinks-PvdA-fractie dringen er op aan om zo snel mogelijk heldere ambities over de overgangstermijn en implementatie op te stellen. Zij menen dat de overheid een rol heeft als marktmeester, en dat een uitgesproken ambitie voor de uitfasering van UZI-middelen als gevolg heeft dat de urgentie en business case voor leveranciers van nieuwe inlogmiddelen groeit. Kan de regering reflecteren op de rol van het Ministerie van VWS als marktmeester en aanjager van technische innovatie op het gebied van inlogmiddelen door het stellen van een heldere overgangstermijn?

Ik onderschrijf het belang van een heldere overgangstermijn voor de uitfasering van UZI-middelen en de invoering van het Dezi-stelsel. Een duidelijke lijn biedt niet alleen richting aan zorgaanbieders, maar creëert ook duidelijkheid en investeringszekerheid voor marktpartijen die veilige, gecertificeerde inlogmiddelen ontwikkelen.

Het ministerie van VWS neemt een actieve rol op zich door wettelijke kaders op te stellen voor het gebruik van inlogmiddelen op het betrouwbaarheidsniveau hoog, en een gefaseerde verplichtstelling in te voeren. Het UZI-register wordt uitgefaseerd en stopgezet per 1 januari 2029.

Deze rol, waarin ik wettelijke kaders stel met een verplichtstelling, draagt bij aan gezonde marktdynamiek en innovatie. Aanbieders van inlogmiddelen weten zo waar ze aan toe zijn. Zij kunnen hun productontwikkeling inrichten op de gestelde eisen en worden daarnaast uitgedaagd tot concurrerende oplossingen op gebruiksgemak en kostenefficiëntie.

De leden van de NSC-fractie merken op dat de Raad van State twee punten van kritiek aanstipt in hun reactie op het voorstel, namelijk het beperken van verplicht gebruik van het nieuwe register tot de SBV-Z en het ontbreken

van een harde deadline voor het verplicht gebruik van goedgekeurde inlogmiddelen voor alle systemen in de zorg. Kan de regering op elk van deze twee punten van advies separaat ingaan?

Het oorspronkelijke wetsvoorstel stelde voor om inlogmiddelen voor het Dezi-stelsel verplicht te maken voor toegang tot de SBV-Z, terwijl ze voor andere toepassingen facultatief zouden zijn. Deze verplichting uit het oorspronkelijke wetsvoorstel zou overeenkomen met de huidige verplichting voor het gebruik van UZI-middelen. Het idee was dat het gebruik van deze inlogmiddelen op termijn vanzelf zou toenemen, aangezien een groot aantal zorgmedewerkers de middelen al in bezit zou hebben. Dit zou het gebruik bij andere toepassingen aantrekkelijk maken, door het beperken van het aantal benodigde inlogmiddelen voor diverse toepassingen en wanneer een zorgmedewerker bij verschillende zorgaanbieders werkt. Bovendien werd een verplichting gezien als een risico voor de noodzakelijke aanpassingen in het complexe landschap van applicaties en systemen.

De Afdeling Advisering van de Raad van State gaf aan dat de bescherming van bijzondere persoonsgegevens zeer belangrijk is en dat de ontwikkelingen in de zorgsector te langzaam gaan. Zij vond dat het wetsvoorstel niet genoeg zou bijdragen om snel te zorgen voor het hoogste betrouwbaarheidsniveau bij toegang tot en uitwisseling van deze gegevens. Daarom adviseerde de Afdeling om een uiterste termijn op te nemen in het wetsvoorstel over wanneer identificatie en inloggen via het Dezi-register, met goedgekeurde inlogmiddelen, verplicht zou moeten zijn voor toegang tot elektronische uitwisselingssystemen en zorginformatiesystemen.

De regering herkent de redenering van de Afdeling advisering van de Raad van State en volgt daarom het advies op. Bij algemene maatregel van bestuur wordt bepaald vanaf welk moment de verplichting in artikel 15, derde lid, van het wetsvoorstel gaat gelden. Deze algemene maatregel van bestuur voorziet in een aanpassing van de Wabvpz door een harde einddatum voor de verplichte aansluiting toe te voegen. Op dit moment is de datum van verplichtstelling op 1 januari 2031 gesteld.

11.1.3Gekwalificeerde elektronische handtekening

11.1.4Goedkeuren inlogmiddelen

11.1.5eIDAS herziening (EDI-wallet)

11.1.6Zorgspecifieke middelen NEN 7518

De leden van de GroenLinks-PvdA-fractie onderstrepen de zorgen over het hanteren van een nog niet bestaande NEN-norm en vragen de regering om bij de publicatie van de norm een korte terugkoppeling te geven aan de Kamer met een zienswijze, en een reactie op wat voor gevolgen dit (mogelijk) heeft voor de implementatie van de wet.

De NEN 7518 was van 24 maart 2025 tot 24 juni 2025 beschikbaar voor publieke consultatie. De norm kon zo breed worden besproken en aangepast op basis van de inbreng. Er zal aan de Kamer een korte terugkoppeling worden gegeven, inclusief de eventuele gevolgen die het mogelijk heeft voor de implementatie van de wet.

11.1.7Zorgmedewerker en het register

De leden van de GroenLinks-PvdA-fractie vragen om een nadere toelichting over hoe zorgmedewerkers worden geïnstrueerd en geïnformeerd over de zorgvuldige omgang met zorggegevens verkregen via een Dezi-nummer.

De Wabvpz schept de randvoorwaarden over hoe zorggegevens veilig en elektronisch mogen worden uitgewisseld of ingezien. Daarnaast wordt de zorgmedewerker bij de registratie in het Dezi-register gewezen op rechten en plichten met betrekking tot het gebruik van het Dezi-register. De zorgmedewerker moet bij zijn registratie akkoord gaan met deze voorwaarden. Deze voorwaarden worden op de website van het Dezi-register gepubliceerd zodat die voor ieder toegankelijk zijn. Tot slot ligt er op basis van de AVG een rol bij de zorgaanbieder om organisatorische maatregelen te nemen om de medewerkers te instrueren over de zorgvuldige omgang met zorggegevens, bijvoorbeeld door middel van bewustwordingscampagnes en handreikingen voor medewerkers.

De leden van de GroenLinks-PvdA-fractie vragen nadere toelichting over de manier waarop burgers toegang kunnen krijgen tot het overzicht van zorgmedewerkers die hun gegevens hebben geraadpleegd of verwerkt.

Burgers kunnen het CIBG vragen om inzicht in de zorgaanbieders die hun gegevens hebben opgevraagd via SBV-Z. Daarnaast heeft iedere burger recht op inzage in hun dossier en de bijbehorende loggegevens bij de zorgaanbieder.

11.1.8Acceptatieplicht inlogmiddelen

11.1.9Gebruiksvriendelijkheid

11.1.10 Implementatie en financiële gevolgen

De leden van de GroenLinks-PvdA-fractie hebben twijfels bij de volgorde om eerst het wetsvoorstel te laten aannemen, voordat er duidelijkheid is over wanneer de UZI-middelen worden uitgefaseerd. Zij zien een duidelijke deadline voor het uitfaseren van UZI-middelen als manier om de urgentie te creëren die nodig is om het ontwikkelen van inlogmiddelen door marktpartijen aan te jagen. Zijn er gesprekken geweest met (mogelijke) leveranciers van de nieuwe inlogmiddelen over de meest effectieve uitfasering en gewenste overgangstijd? Zo nee, kunnen zij worden betrokken bij de gesprekken die het Ministerie van VWS heeft met het zorgveld op dit punt?

De regering begrijpt de zorgen over de volgorde waarin eerst het wetsvoorstel wordt behandeld, terwijl de uitfasering van UZI-middelen tegelijkertijd onderwerp van aandacht is. De regering wijst erop dat inmiddels is vastgesteld dat de uiterste deadline voor het gebruik van UZI-middelen is bepaald op 1 januari 2029. Daarmee is het wettelijk kader helder en wordt het noodzakelijke perspectief geboden aan marktpartijen en zorgaanbieders. Een duidelijke deadline is van essentieel belang om urgentie te creëren en de ontwikkeling van nieuwe, gecertificeerde inlogmiddelen door marktpartijen te stimuleren. Leveranciers hebben aangegeven dat voorspelbaarheid en onomkeerbaarheid van de verplichtstelling belangrijk zijn om investeringen in innovatie en certificering rendabel te maken.

De leden van de GroenLinks-PvdA-fractie vragen hoe de regering volgens deze (mogelijke) leveranciers het beste de concurrentie kan aanjagen en ondernemers in staat stellen om zo snel mogelijke goede inlogmiddelen te bouwen? Wordt hierbij ook de bewindspersoon van Economische Zaken betrokken?

Er zijn verkennende gesprekken gevoerd met (potentiële) leveranciers over de implementatiestrategie en de effectieve stimulering van de markt. Leveranciers worden ook actief betrokken bij de verdere uitwerking van de implementatieaanpak, zodat hun inzichten benut kunnen worden om de concurrentie te bevorderen en een breed aanbod van kwalitatieve, gebruiksvriendelijke inlogmiddelen te realiseren.

De Minister van Economische Zaken en Klimaat is niet betrokken bij dit traject. De verantwoordelijkheid voor het stelsel, de wetgeving en de marktdynamiek ligt volledig bij mijn ministerie.

De leden van de NSC-fractie delen de zorg van experts in het veld dat binnen een aantal jaar kwantumcomputers in staat zullen zijn de huidige vormen van encryptie te verbreken en zo bij gevoelige persoonsgegevens zouden kunnen komen. Deze leden vragen hoe toekomstbestendig de beveiliging van persoonsgegevens onder het stelsel van de wetswijziging is. Is het Dezi-register kwantumveilig? Zo nee, welke stappen is regering van plan te nemen om de beveiliging van de persoonsgegevens ook toekomstbestendig te houden?

Het is onduidelijk wanneer de kwantumcomputer daadwerkelijk beschikbaar komt, maar dat zal niet binnen paar jaar zijn. Er is op dit moment ook nog geen nieuwe standaard voor encryptie beschikbaar. Wel bereidt het ministerie van VWS zich actief voor op de komst van kwantumcomputers. Zo werken wij als ministerie samen met andere ministeries om met de industrie nieuwe vormen van encryptie te ontwikkelen die bestand zijn tegen kwantumcomputers.

11.2 Uitvoeringstoets CIBG

De leden van de GroenLinks-PvdA-fractie lezen met interesse over de zorgen van het CIBG. Als uitvoerende organisatie weegt haar analyse zwaar. Kan concreet worden gemaakt hoe de regering de zorgen over de uitdagingen rondom de nog te ontwikkelen regelgeving heeft weggenomen? Hoe gaat de regering de uitdagingen naar haar zeggen «uitvoerbaar» maken? Kan het CIBG bevestigen dat er voldoende is tegemoetgekomen aan haar zorgen?

De regelgeving omtrent het toekennen van autorisatiekenmerken aan inlogmiddelen is op het moment van schrijven nog niet definitief. De regels hieromtrent volgen onder andere uit de uitvoeringshandelingen

op grond van de vernieuwde eIDAS-verordening.[38] Op het moment van beantwoording van deze Kamervragen zijn deze handelingen nog niet gepubliceerd. Ook worden er nog nadere normeringen verwacht vanuit bijvoorbeeld het Europees Telecommunicatie en Standaardisatie instituut (ETSI).

De lagere regelgeving zal in goede afstemming met het CIBG worden opgesteld. Ik zal goed een vinger aan de pols houden zodra dit wetsvoorstel in werking is getreden. Zodra deze regelgeving definitief is en mogelijke uitdagingen inzichtelijk zijn, dan zal het ministerie van VWS tezamen met het CIBG bezien hoe deze uitvoerbaar wordt gemaakt, dit zou bijvoorbeeld kunnen met beleidsregels. Met deze werkwijze wordt er voor het CIBG voldoende tegemoetgekomen aan de geuite zorgen.

De leden van de GroenLinks-PvdA-fractie vragen om de afbakening van de taken binnen het nieuwe Dezi-afsprakenstelsel met spoed vast te leggen en aan de Kamer te doen toekomen.

De rollen binnen het Dezi-stelsel alsmede de afbakening van taken binnen deze rollen worden op dit moment uitgewerkt. Zodra deze zijn vastgelegd zullen deze aan de Kamer worden gestuurd.

11.3 Toezicht- en Handhaafbaarheidstoets IGJ

De leden van de GroenLinks-PvdA-fractie vragen te bevestigen dat er naar wens is tegemoetgekomen aan de zorgen van de IGJ. Zijn de processen en definitiebepalingen nu voldoende duidelijk voor IGJ?

De IGJ heeft aangeven dat haar feedback in de toezicht- en handhaafbaarheidstoets over de processen en definitiebepalingen voldoende zijn overgenomen en aangepast in het wetsvoorstel en de memorie van toelichting.

De leden van de GroenLinks-PvdA-fractie vragen of de regering de ondersteunende rol die het IGJ «mogelijk» zal spelen duidelijker kan definiëren.

De IGJ kan een inschatting maken omtrent de mate waarin de intrekking van een inlogmiddel de kwaliteit van zorg kan beïnvloeden. In een zeer uitzonderlijk geval kan de IGJ haar bevoegdheden inzetten om te bewerkstelligen dat de betreffende zorgaanbieder informatie verschaft, of kan zij hem ertoe te bewegen maatregelen te treffen om de inlogmiddelen te vervangen zodat de continuïteit van de zorg niet in gevaar komt. De IGJ verwacht dat een dergelijke situatie zich doorgaans niet zal voordoen, omdat zorgaanbieders normaliter zelf en in goed overleg al de benodigde maatregelen treffen.

11.4 Advies Adviescollege toetsing regeldruk (ATR)

11.5 Advies Autoriteit Persoonsgegevens (AP)

De leden van de PVV-fractie vragen in hoeverre de zorgen en aanbevelingen van de Autoriteit Persoonsgegevens en andere stakeholders zijn meegenomen in de uiteindelijke opmaak van de wet.

De Autoriteit Persoonsgegevens heeft advies gegeven over het wetsvoorstel. Dit advies is zorgvuldig verwerkt in de verdere uitwerking van het wetsvoorstel en daarvan is een verantwoording opgenomen in de memorie van toelichting. Wanneer de algemene maatregel van bestuur gereed is, dan wordt dit ook voor advisering voorgelegd aan de Autoriteit Persoonsgegevens om ervoor te zorgen dat de implementatie aansluit bij de geldende privacy-kaders.

De leden van de PVV-fractie vragen of er ruimte is voor uitzonderingen of maatwerk in specifieke situaties, bijvoorbeeld bij kleinschalige zorgaanbieders of kwetsbare groepen.

Er is bewust ruimte gecreëerd voor maatwerk in specifieke situaties. Kleinschalige zorgaanbieders en kwetsbare groepen krijgen voldoende tijd om de overstap te maken, waarbij ondersteuning beschikbaar is via standaardoplossingen en praktische handreikingen. Op deze manier wordt ervoor gezorgd dat de nieuwe regelgeving voor alle partijen uitvoerbaar blijft, zonder concessies te doen aan de veiligheid en betrouwbaarheid van digitale toegang.

De leden van de GroenLinks-PvdA-fractie vragen de regering om te bevestigen dat de zorgen van de Autoriteit Persoonsgegevens naar wens zijn overgenomen. Genoemde leden zijn van mening dat het enkel beschrijven van

[38] 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.

de risico's genoemd door de AP, zoals gedaan in paragraaf 6.8, onvoldoende duidelijkheid geeft over hoe deze risico's gemitigeerd dienen te worden. Zij vragen om samen met de AP te verkennen hoe de regering deze risico's daadwerkelijk kan mitigeren.

De AP heeft advies gegeven over het wetsvoorstel. Dit advies is zorgvuldig verwerkt in de verdere uitwerking van het wetsvoorstel en daarvan is verantwoording opgenomen in de memorie van toelichting. Zodra de algemene maatregel van bestuur gereed is, zal dit opnieuw ter advisering worden voorgelegd aan de AP om ervoor te zorgen dat de implementatie aansluit bij de geldende privacy-kaders.

De risico's die de AP in haar advies heeft benoemd, zoals verwoord in paragraaf 6.8 van de memorie van toelichting, zijn zorgvuldig geanalyseerd en meegenomen in de verdere uitwerking van het wetsvoorstel. Het enkel beschrijven van deze risico's is bedoeld om transparant te zijn over de mogelijke aandachtspunten. Het mitigeren van deze risico's is meegenomen en verwerkt in het wetsvoorstel.

II. Artikelsgewijze toelichting

Artikel I: Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

De leden van de PVV-fractie hebben naar aanleiding van artikel 1 de volgende vraag. Bij artikel 10.2 wordt een lid toegevoegd, onder punt 5: Hier wordt de datum, 1 januari 2028 genoemd voor de toepassing op de uitgegeven middelen. Echter bij het nieuwe artikel 18 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg staat 1 januari 2029 als datum vermeld. Waarom wordt hier een andere datum vermeld?

Het is niet de bedoeling dat er een discrepantie zit in de data. Artikel I onder D van het wetsvoorstel ziet op een wijzing van de Wabvpz. Artikel II onder B ziet op een wijziging van artikel 10.2 van de Jeugdwet. Beide artikelen horen te gaan over een eerbiedigende werking van de geldende regeling tot 1 januari 2029. Dit betreft een scherp opgemerkte typefout, die eerder al is opgemerkt. De datum van Artikel II onder B pas ik middels een nota van wijziging aan naar 1 januari 2029.

Onderdeel A – Artikel 1 (begripsbepaling)

De leden van de GroenLinks-PvdA-fractie hebben vragen over de definitie bepalingen. Zij vragen om toe te lichten of en hoe de definities achteraf nog nader ingevuld kunnen worden, bijvoorbeeld door een definitie te verbreden, te versmallen, of te nuanceren.

Zolang een voorstel van wet nog niet is aangenomen, kan het door de regering dan wel een of meer leden van uw Kamer worden gewijzigd. In deze fase is het dus mogelijk definities te verbreden, te versmallen, of te nuanceren. Wanneer een wetvoorstel is aangenomen, is een wetswijziging nodig om een definitie aan te passen.

Onderdeel B – Artikel 14 – Het register van zorgaanbieders, zorgmede-werkers, indicatieorganen en zorgverzekeraars

De leden van de GroenLinks-PvdA-fractie vragen of in dit artikel de mogelijkheid is opgenomen om een bepaling toe te voegen die voorschrijft om in het verwerken van persoonsgegevens een zo zorgvuldig mogelijke verwerking middels de best beschikbare technieken te betrachten. Heeft een dergelijke wettelijke bepaling volgens de regering meerwaarde?

Een bepaling die voorschrijft om in het verwerken van persoonsgegevens een zo zorgvuldig mogelijke verwerking middels de best beschikbare technieken te betrachten, biedt geen meerwaarde. Artikel 14 van het wetsvoorstel kent al voldoende waarborgen om de verwerking van persoonsgegevens zo goed mogelijk te beschermen. De verzochte persoonsgegevens van zorgaanbieders, zorgmedewerkers, indicatieorganen of zorgverzekeraars voor inschrijving in het register zijn al beperkt tot een minimum. Daarnaast wordt voor het verkrijgen van een Dezi-nummer een betrouwbare koppeling gemaakt met het BSN van de medewerker.

Onderdeel B – Artikel 14a – Goedkeuring inlogmiddelen

De leden van de GroenLinks-PvdA-fractie wijzen erop dat de uitwerking via algemene maatregelen voor bestuur de precieze uitvoering van het wetsvoorstel moeilijk controleerbaar maakt. Zij vragen om zo snel als mogelijk duidelijkheid te bieden of contouren te delen van de nadere uitwerking. Op welke termijn na de invoering van de wet wordt de algemene maatregel van bestuur aan de Kamer verzonden?

Op dit moment bereid ik nog de algemene maatregel van bestuur voor, die een nadere invulling geeft van het wetsvoorstel. Het is mijn streven om de algemene maatregel van bestuur aan het einde van de zomer of aan het begin van het najaar in internetconsultatie te brengen, dan is deze openbaar en in te zien. Ik kan uw Kamer toezeggen deze algemene maatregel van bestuur u dan ter informatie te doen toekomen, zodat het, indien u dat wenst, kan worden betrokken bij de plenaire behandeling van het wetsvoorstel. Overigens wordt deze algemene maatregel van bestuur voorgehangen bij beide Kamers.

De leden van de GroenLinks-PvdA-fractie vragen naar de overweging om geen papieren / analoge mogelijkheden per wet toe te staan. Is het beschikbaar stellen van analoge alternatieven niet een noodzakelijke terugvaloptie, mocht er sprake zijn van een brede storing? Deze leden vragen voorts of de regering het niet noodzakelijk is om de mogelijkheid voor analoge alternatieven per wet toe te staan, om de continuïteit van zorgverlening in het geval van een storing te waarborgen? Tot slot vragen deze leden hoe deze wet bijdraagt aan het cyberweerbaar maken van Nederland?

Het ondersteunen van papieren aanvragen voor registratie wordt als niet kosteneffectief en administratief belastend beschouwd. Daarnaast beoog ik met het Dezi-register juist dat de zorg verder gaat digitaliseren op een veilig betrouwbaarheidsniveau. Het handmatig laten invullen van formulieren en door behandelaren laten verwerken sluit hier niet op aan en introduceert tevens een risico op fouten.

Om de continuïteit van deze dienstverlening te garanderen, worden er maatregelen getroffen, zoals hoge beschikbaarheidsafspraken met de leveranciers, dubbele uitvoering in de gebruikte techniek en bedrijfscontinuïteitsplannen die periodiek worden getest.

De organisaties in de zorg (naast organisaties in andere sectoren) moeten digitaal weerbaar zijn om in de nabije toekomst te voldoen aan de Cyberbeveiligingswet, zodat zoveel mogelijk wordt voorkomen dat de continuïteit van de zorg gevaar loopt door cyberaanvallen. Door de Cyberbeveiligingswet wordt er op digitale kwetsbaarheden gemonitord. Het in kaart brengen van deze kwetsbaarheden betekent dat er sneller kan worden opgetreden.

Onderdeel D – Artikel 18 (overgangsrecht)

De leden van de GroenLinks-PvdA-fractie vragen of er alternatieve termijnen voor de overgangsperiode zijn overwogen. Graag een toelichting wat de gevolgen zijn van een kortere of langere overgangsperiode?

Er is overwogen om de overgangsperiode korter dan wel langer vorm te geven. Een kortere overgangsperiode houdt voor zorgaanbieders in dat de UZI-middelen, die op dit moment met een driejarige geldigheid worden uitgegeven, korter gebruikt kunnen worden. Een kortere periode impliceert ook dat zorgaanbieders die nu UZI-middelen gebruiken eerder moeten migreren naar middelen uit het Dezi-stelsel.

Een langere overgangsperiode kan een negatieve werking hebben op de ontwikkeling van zorgspecifieke middelen. Ook impliceert een langere periode dat voor het uitgeven van UZI-middelen er een Europese aanbesteding moet worden uitgeschreven, waarvan op voorhand duidelijk is dat de kosten niet in verhouding staan tot de duur van het verlengen van deze periode.

Artikel III: Overgangsrecht

De leden van de CDA-fractie vragen waarom ervoor gekozen is om het precieze moment waarop de verplichting om gebruik te maken van inlogmiddelen met betrouwbaarheidsniveau «hoog» vast te leggen in een algemene maatregel van bestuur en niet in de wet zelf.

De keuze om de verplichting van het gebruik te maken van inlogmiddelen met betrouwbaarheidsniveau hoog per algemene maatregel van bestuur te regelen is omdat het een betere mogelijkheid biedt voor een realistische implementatietermijn voor de afzonderlijke inlogmiddelen. Hierdoor wordt maatwerk mogelijk gemaakt.

De minister van Volksgezondheid,
Welzijn en Sport,

J.A. Bruijn