AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 088 0712 140
autoriteitpersoonsgegevens.nl

De Minister van Volksgezondheid, Welzijn en Sport
Postbus 20350
2500 EJ DEN HAAG

Datum	Ons kenmerk	Uw brief van
28 november 2023	z2023-02938	14 juli 2023
	Contactpersoon	Uw kenmerk
		3636519-1051026-DICIO

Onderwerp
Advies over het concept wetsvoorstel DIAZ

Geachte heer Kuipers,

Bij brief van 14 juli 2023 is de Autoriteit Persoonsgegevens (AP) op grond van het bepaalde in artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (AVG), geraadpleegd over het concept voor wijziging van de Wet aanvullende bepalingen verwerkingen persoonsgegevens in de zorg (Wabvpz) in verband met digitale identificatie en authenticatie in de zorg (hierna: het concept).

De AP heeft bezwaar tegen het concept met betrekking tot het voorgestelde artikel 14 en 15 en adviseert de procedure niet voort te zetten tenzij het bezwaar is weggenomen (paragraaf 1). Daarnaast geeft het concept de AP nog aanleiding tot het maken van enkele opmerkingen (paragraaf 2 tot en met 5).

Hoofdlijn van het advies

- Met het concept beoogt de minister zorgaanbieders en zorgmedewerkers te stimuleren om voor toegang tot elektronische uitwisselingssystemen en zorginformatiesystemen inlogmiddelen te gebruiken die voldoen aan betrouwbaarheidsniveau hoog. Alhoewel de AP die inzet toejuicht, is naar oordeel van de AP krachtiger overheidsoptreden op zijn plaats.
- Ten eerste omdat in de praktijk nog onvoldoende geschikte inlogmiddelen op betrouwbaarheidsniveau hoog beschikbaar zijn. De AP is niet overtuigd dat die er uit eigen beweging van het veld in de nabije toekomst wel zullen zijn. Ten tweede omdat het concept het gebruik van inlogmiddelen op betrouwbaarheidsniveau hoog niet verplicht stelt, behalve voor toegang tot SBV-Z.[1]

[1] Met SBV-Z (Sectorale Berichten Voorziening in de Zorg) kunnen ingeschrevenen het BSN van een patiënt uit de Basisregistratie Personen (BRP) opvragen of verifiëren. Zie artikel 3 Wet algemene bepalingen burgerservicenummer (Wabb) en sbv-z.nl/over-ons.

- De AP adviseert in het concept een concrete termijn op te nemen vanaf wanneer zorgaanbieders en zorgmedewerkers verplicht gebruik dienen te maken van goedgekeurde inlogmiddelen met betrouwbaarheidsniveau hoog om toegang te krijgen tot elektronische uitwisselingssystemen en zorginformatiesystemen. Zolang die inlogmiddelen in de praktijk niet geschikt of beschikbaar zijn, is het naar oordeel van de AP aan de minister om er voor te zorgen dat er in ieder geval één inlogmiddel is dat voldoet aan betrouwbaarheidsniveau hoog en geschikt is om in de praktijk te worden gebruikt.
- Daarnaast heeft de AP opmerkingen over maatregelen die het gebruiksgemak verhogen maar tegelijkertijd het beveiligingsniveau kunnen verlagen (adviespunt 2.1), over het risico bij gebruik van privételefoons (adviespunt 2.2), over het toelaten van zorgmedewerkers tot het register (adviespunt 3), over toegang tot andere diensten dan elektronische uitwisselingssystemen en zorginformatiesystemen (adviespunt 4.1), over de koppeling van HR-systemen (adviespunt 4.2), over de te grote nadruk op gegevensuitwisseling (5.1) en over de verruiming van bevoegdheden van de IGJ (adviespunt 5.2).

Strekking van het concept

Voor zorgaanbieders, indicatieorganen en zorgverzekeraars bestaan momenteel afzonderlijke UZI-registers[2] waarin zij op verzoek kunnen worden ingeschreven.[3] Eenmaal ingeschreven, kunnen zij een UZI-pas[4] of een UZI-servercertificaat[5] (samen: UZI-middelen) aanvragen waarmee toegang kan worden verkregen tot SBV-Z.[6] Daarnaast kan met de UZI-middelen toegang worden verkregen tot het Landelijk Schakelpunt (LSP) en enkele diensten zoals het Landelijk Implantatenregister en communicatieknooppunt VECOZO.[7] Het bezit van een UZI-pas alleen is niet voldoende om zonder meer toegang te krijgen tot zorginformatie. Er moet ook autorisatie plaatsvinden.[8] Bovendien is enkel het aanbieden van de pas niet voldoende, daarnaast moet ook een pincode worden ingevoerd.[9]

Hoofdzakelijk worden in de memorie van toelichting drie problemen genoemd met betrekking tot de huidige praktijk. Ten eerste bestaat momenteel geen grondslag voor het gebruik van het UZI-registers en UZI-middelen voor andere diensten dan SBV-Z. Ten tweede ervaart de praktijk verschillende problemen

[2] Unieke Zorgverlener Identificatie Register; Het UZI-register wordt beheerd bij het CIBG, een onderdeel van het ministerie van VWS.
[3] Artikel 14, eerste lid, Wabvpz.
[4] De UZI-pas wordt uitgegeven aan personen en bevat een chip waar de zorgidentiteit van de ingeschrevene fysiek op staat geprint. De UZI-pas wordt uitgelezen met een kaartlezer. De gegevens op de chip zijn blijkens memorie van toelichting (MvT) p. 13 de zogenaamde UZI-attributen: wie ben je = unieke zorgidentificatienummer of UZI-nummer, waar werk je = unieke registratie abonneenummer of URA-nummer, wat zijn je bevoegdheden = rolcode die aangeeft welke bevoegdheden een zorgprofessional heeft.
[5] Het UZI-servercertificaat wordt door het CIBG uitgegeven aan systemen en betreft een computerbestand dat voldoet aan de normen van de Public Key Infrastructure voor de overheid (PKI-o). Met het certificaat kan een website, applicatie of server aantonen dat deze bij een UZI-register ingeschreven organisatie hoort; Zie ook: logius.nl/domeinen/toegang/pkioverheid/hoe-werkt-het.
[6] Artikel 15, derde lid, Wabb.
[7] Zie: bronnen.zorggegevens.nl/Bron?naam=Unieke-Zorgverlener-Identificatie-Register. Het betreft o.a. ook de Beveiligde Registratie Bijzondere Assets, het portaal Hulpverleners Kunnen Verklaringen Invoeren en het Nationaal Contactpunt voor e-Health.
[8] Authenticatie gaat over de vraag wie iemand is. Autorisatie gaat over de vraag bij welke informatie iemand mag. Zie ook: uziregister.nl/uzi-pas/waarvoor-heeft-u-een-uzi-pas-nodig/authenticatie en MvT p. 11.
[9] Zo blijkt uit navraag bij het ministerie.

met de UZI-pas,[10] en ten derde voldoen andere inlogmiddelen vaak niet aan het hoogste betrouwbaarheidsniveau[11] van de eIDAS-verordening[12] terwijl dat gelet op artikel 5, eerste lid, onder f, AVG wel vereist is.[13] Met het concept wordt beoogd deze problemen als volgt op te lossen:

1 Met de nieuwe inlogmiddelen kunnen ingeschrevenen naast SBV-Z[14] ook toegang krijgen tot elektronische uitwisselingssystemen en zorginformatiesystemen.[15] Dat geldt alleen voor zorgaanbieders en zorgmedewerkers, en dus niet voor zorgverzekeraars en indicatieorganen.[16]
2 Met het concept stopt het CIBG met het uitgeven van UZI-middelen,[17] en naast fysieke passen en servercertificaten kunnen nu ook andere inlogmiddelen worden gebruikt, mits de minister van VWS daarvoor goedkeuring verleent.[18] De uitfasering van UZI-middelen begint per 2025 zodat het zorgveld tot uiterlijk 2028 heeft om over te stappen op een nieuw middel.[19]
3 Voorwaarde daarvoor is dat het middel, en indien van toepassing de koppeling van dit middel aan een ingeschrevene, voldoet aan het betrouwbaarheidsniveau hoog.[20] Dat een inlogmiddel voldoet aan het betrouwbaarheidsniveau hoog kan worden aangetoond door het overleggen van een bewijsmiddel.[21] Beoogd wordt bij AMvB in ieder geval drie verschillende bewijsmiddelen aan te wijzen die kunnen leiden tot goedkeuring:[22]
   - Publieke en private, Nederlandse en buitenlandse, identificatiemiddelen[23] die onder de Wdo zijn erkend.[24]

[10] Genoemd worden de kosten, het risico op uitlenen, de ongeschiktheid voor gebruik op mobiele apparaten, en het feit dat telkens een nieuwe pas moet worden gemaakt als er een wijziging plaatsvindt in werkgever-werknemer relatie of beroep.
[11] Artikel 8, tweede lid, eIDAS omschrijft drie betrouwbaarheidsniveaus voor stelsels van elektronische identificatie, die een (1) beperkte, (2) substantiële of (3) hogere mate van vertrouwen bieden in iemands opgegeven of beweerde identiteit. Voor elk betrouwbaarheidsniveau bestaan op grond van artikel 8, derde lid, eIDAS jo. artikel 1 en bijlage Uitvoeringsverordening eIDAS (EU) Nr. 2015/1502 minimale technische specificaties en procedures. Zie ook: https://www.avghelpdeskzorg.nl/onderwerpen/eidas.
[12] 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. Nationale regels hierover worden vastgesteld in de Wet digitale overheid (Wdo).
[13] MvT p. 16.
[14] Voorgesteld artikel 14a, eerste lid, Wabvpz.
[15] Voorgesteld artikel 14a, tweede lid, Wabvpz; Voorgesteld artikel 14a, vierde lid, onder a, Wabvpz.
[16] MvT p. 10.
[17] Daarmee is CIBG niet langer Trusted Service Provider (TSP) onder het PKI-o-stelsel. Die taak zal worden overgenomen door andere TSP's die moeten voldoen aan de eisen om PKI-o middelen uit te geven, zie MvT p. 15. Voor wat betreft de uitgifte van zorgspecifieke middelen dient zowel de leverancier van een middel als de zorgaanbieder of koepelorganisatie die dat middel uitgeeft (dat kan ook de leverancier zelf zijn) aan de zorgmedewerkers, te zijn gecertificeerd onder NEN 7518. Zie MvT p. 15.
[18] Voorgesteld artikel 15, eerste lid, Wabvpz; In de praktijk zal het CIBG belast worden met de taak om goedkeuring van de inlogmiddelen te verlenen, zo blijkt uit p. 22 MvT.
[19] MvT p. 23.
[20] Voorgesteld artikel 15, eerste lid, Wabvpz.
[21] MvT p. 12.
[22] Voorgesteld artikel 15, tweede lid, onder a-e, Wabvpz.
[23] Artikel 1 Wdo: '[Een] *elektronisch middel dat persoonsidentificatiegegevens bevat en gebruikt wordt voor de authenticatie van een natuurlijke persoon, rechtspersoon of onderneming die toegang wenst tot elektronische dienstverlening*'.
[24] Artikel 9 Wdo, dat strekt tot de toelating van identificatiemiddelen en diensten, is nog niet in werking getreden. DigiD is een voorbeeld van een publiek identificatiemiddel dat onder de Wdo is erkend.

- Certificering van zorgspecifieke middelen[25] onder de NEN 7518[26].[27]
- PKI-o-certificering (voorzetting van de UZI-servercertificaten).

Daarnaast wordt in plaats van afzonderlijke UZI-registers voor zorgaanbieders, indicatieorganen en zorgverzekeraars nu één register ingesteld.[28] Aan dat register wordt ook een nieuwe categorie 'zorgmedewerker'[29] toegevoegd. Zorgmedewerkers kunnen zich laagdrempelig inschrijven in het UZI-register bij het CIBG. Daarna verifieert de zorgaanbieder of de zorgmedewerker bij hem werkzaam is en of hij toegang moet kunnen krijgen tot SBV-Z of andere systemen die de zorgaanbieder gebruikt. Als de zorgmedewerker niet meer werkzaam is bij de zorgaanbieder, blijft hij ingeschreven in het UZI-register maar verliest hij de toegang tot die systemen.[30] Bij de koppeling van een zorgspecifiek inlogmiddel aan een ingeschrevene verwerkt de zorgaanbieder het BSN van de ingeschrevene.[31]

Advies

1. Krachtiger overheidsoptreden vereist

Op grond van artikel 32 AVG zijn verwerkingsverantwoordelijken en verwerkers verplicht om passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Omdat gegevens over gezondheid bijzondere persoonsgegevens[32] zijn, wordt aan de beveiliging van die gegevens zwaardere eisen gesteld dan aan andere persoonsgegevens. In gevallen waar het gaat om gegevens waar het medisch beroepsgeheim van de zorgverlener op rust, heeft de AP in het kader van authenticatie van patiënten voor toegang tot patiëntportalen regelmatig aangegeven dat daarvoor het 'hoogste betrouwbaarheidsniveau' is vereist.[33] In de terminologie van de eIDAS-verordening dient een inlogmiddel dan te voldoen aan betrouwbaarheidsniveau 'hoog'.

---

[25] Blijkens MvT p. 13 gaat het om elektronische middelen voor identificatie en authenticatie die onder de verantwoordelijkheid van een zorgaanbieder wordt uitgereikt aan zijn zorgmedewerkers, zoals een ziekenhuispas (ook wel personeelspas) of een digitale wallet. Digitale wallets worden in de MvT gedefinieerd als *'inlogmiddelen die de zorgidentiteit uit het UZI-register in de 'wallet' opslaan en daarmee niet met iedere inlog langs het UZI-register gaan'*, MvT p. 27.

[26] De NEN 7518 (Identificatie & Authenticatie) is nog in ontwikkeling. Verwachte publicatie eind 2023, zie gegevensuitwisselingindezorg.nl/actueel/nieuws/2023/05/08/overzicht-ontwikkeling-nen-normen-wegiz.

[27] '*Om voor goedkeuring in aanmerking te komen moet het certificaat van een zorgspecifieke middel zijn verstrekt door een* [certificerende instelling] *die door de* [Raad voor Accreditatie] *is geaccrediteerd'*, MvT p. 13.

[28] Voorgesteld artikel 14, derde lid, onder a-d, Wabvpz.

[29] In het voorgestelde artikel 1 Wabvpz, onder een nader te bepalen onderdeelnummer, als volgt gedefinieerd: '*eenieder die werkzaamheden verricht of gaat verrichten voor een zorgaanbieder en daarbij cliëntgegevens raadpleegt met behulp van een goedgekeurd inlogmiddel*. Onder 'inlogmiddel' wordt op grond van dezelfde bepaling begrepen: '[een] *elektronisch middel voor identificatie en authenticatie ten behoeve van elektronische gegevensuitwisseling in de zorg*'.

[30] MvT p. 11-12.

[31] Voorgesteld artikel 14a, derde lid, Wabvpz. Voor de uitgifte van een middel dat erkend is op grond van de Wdo bestaat deze grondslag al op grond van artikel 16 Wdo; De wettelijke grondslag voor verwerking van het BSN geldt alleen voor zorgaanbieders. Voorzien is dat andere uitgevers van zorgspecifieke middelen een contract aangaan met zorgaanbieders. Daarmee zijn zorgaanbieders verwerkingsverantwoordelijk en zijn uitgevers, anders dan zorgaanbieders zelf, verwerker. Zie MvT p. 20.

[32] Artikel 9 van de AVG.

[33] Brief van de AP aan het ministerie van VWS van 4 oktober 2018 betreffende patiëntauthenticatie (z2018-17577) en Brief van de AP aan de NVZ Nederlandse Vereniging van Ziekenhuizen van 7 oktober 2016.

In het concept wordt ook voor authenticatie van zorgaanbieders en zorgmedewerkers ingezet op betrouwbaarheidsniveau hoog.[34] De AP onderschrijft het belang daarvan, en juicht het initiatief van de regering om het veld richting dat doel te bewegen dan ook sterk toe.

Volledigheidshalve merkt de AP op dat het gebruik van een inlogmiddel met betrouwbaarheidsniveau hoog op zichzelf niet betekent dat een organisatie alle vereiste passende technische en organisatorische maatregelen heeft getroffen. Het gebruik van een dergelijk inlogmiddel kan evenwel onderdeel zijn van de maatregelen die getroffen moeten worden. De AP benadrukt daarom dat naast de eisen die de eIDAS-verordening stelt aan betrouwbaarheidsniveau hoog, er ook andere maatregelen kunnen zijn die verwerkingsverantwoordelijken en verwerkers op grond van artikel 32 AVG moeten treffen.

De AP stelt voorop dat het in de eerste plaats aan de verwerkingsverantwoordelijke zelf is om op grond van artikel 32, eerste lid, AVG passende technische en organisatorische maatregelen te treffen om aan het vereiste beveiligingsniveau te voldoen. In de MvT wordt echter aangegeven dat de zorgsector vandaag nog "*veel verschillende inlogmethoden gebruikt die vaak niet aan het vereiste betrouwbaarheidsniveau hoog voldoen*".[35] Dat is voldoende aanleiding om te concluderen dat krachtiger overheidsoptreden op zijn plaats is. Naar oordeel van de AP schieten de voornemens daarin tekort.

Dat heeft er in de kern mee te maken dat, zo blijkt uit aanvullende informatie die het ministerie aan de AP heeft verstrekt, in de praktijk nog onvoldoende geschikte inlogmiddelen op betrouwbaarheidsniveau hoog beschikbaar zijn, en het er ook niet op lijkt dat die er in de nabije toekomst wel zullen zijn. Het veld verkeert al jaren onder de verantwoordelijkheid om inlogmiddelen te gebruiken die voldoen aan het hoogste betrouwbaarheidsniveau maar heeft dat, zo blijkt, onvoldoende gedaan. Met dit concept wordt daar niet alleen niets aan veranderd, zorgaanbieders mogen namelijk nog steeds zelf kiezen of ze wel of niet een goedgekeurd inlogmiddel gebruiken, de UZI-middelen die wel al aan betrouwbaarheidsniveau hoog voldoen zullen ook nog worden uitgefaseerd. Daarmee verliest de zorgsector dus een belangrijk inlogmiddel dat, alhoewel niet ideaal, wel werkt, veilig is en in de praktijk momenteel de standaard is voor toegang het LSP, het Landelijk Implantatenregister en VECOZO. Óf en wanneer daar een goed inlogmiddel voor in de plaats komt is een groot vraagteken. Dit acht de AP onwenselijk.

Daarnaast is het concept naar oordeel van de AP te vrijblijvend. Het laten goedkeuren van inlogmiddelen wordt zoals gezegd niet verplicht gesteld, behalve voor toegang tot SBV-Z. Uit navraag bij het ministerie blijkt echter dat toegang tot SBV-Z veelal wordt verkregen via servercertificaten, niet door in te loggen met bijvoorbeeld een pas of wallet. Het risico bestaat dus dat het concept een lege huls wordt. Daarbij maken de kosten die zorgaanbieders moeten maken om hun bestaande inlogmiddelen te certificeren, aan te passen of om nieuwe inlogmiddelen aan te schaffen, het niet aantrekkelijk voor zorgaanbieders om die stap te maken. Dat geldt des te meer voor middelgrote en kleine zorgaanbieders.

Gelet op de ernst van de huidige praktijk en het belang van betrouwbare authenticatie voor toegang tot gegevens over gezondheid, acht de AP het noodzakelijk dat de minister meer maatregelen neemt om te

[34] MvT p. 8.
[35] MvT p. 8.

waarborgen dat de zorgsector binnen een redelijke termijn overstapt op het gebruik van inlogmiddelen met betrouwbaarheidsniveau hoog. Ten eerste is van belang dat daarvoor een concrete termijn in de wet wordt opgenomen, na verloop waarvan de sector verplicht wordt gebruik te maken van goedgekeurde inlogmiddelen met betrouwbaarheidsniveau hoog. Als die inlogmiddelen er niet zijn, is het naar oordeel van de AP aan de minister om te garanderen dat er ten tijde van inwerkingtreding van de verplichting in ieder geval één inlogmiddel is dat aan het vereiste betrouwbaarheidsniveau voldoet en geschikt is om in de praktijk te worden gebruikt. Bijvoorbeeld door de ontwikkeling van een dergelijk middel bij het CIBG te beleggen, door de productie van de huidige UZI-middelen in stand te houden of door een private partij in dienst te nemen die die taak op zich neemt.

De AP adviseert in het concept een concrete termijn op te nemen vanaf wanneer zorgaanbieders en zorgmedewerkers verplicht gebruik dienen te maken van goedgekeurde inlogmiddelen met betrouwbaarheidsniveau hoog om toegang te krijgen tot elektronische uitwisselingssystemen en zorginformatiesystemen. Zolang die inlogmiddelen in de praktijk niet geschikt of beschikbaar zijn, is het naar oordeel van de AP aan de minister om er voor te zorgen dat er in ieder geval één inlogmiddel is dat voldoet aan betrouwbaarheidsniveau hoog en geschikt is om in de praktijk te worden gebruikt.

2. Contra-effectieve maatregelen

2.1 Omzeiling hoger betrouwbaarheidsniveau

Inloggen met de sterkere authenticatie zal naar inschatting van het ministerie enkele seconden langer duren. Om dat te compenseren stelt het ministerie voor dat authenticatie bijvoorbeeld slechts één keer per dag hoeft, en ook buiten het zorgproces om gevraagd kan worden. Daarnaast wordt gesuggereerd om bijvoorbeeld de frequentie van het inloggen op verschillende zorgapplicaties terug te brengen.[36]

De AP waarschuwt voor de beveiligingsrisico's die met dit soort maatregelen gepaard kunnen gaan. Als maar eenmaal per dag met betrouwbaarheidsniveau hoog hoeft te worden ingelogd, blijft het ook mogelijk om dat middel gedurende de dag aan iemand anders te geven. Die ander hoeft dan blijkbaar geen gebruikersnaam, wachtwoord of iets dergelijks op te geven.

De AP adviseert de passages uit de MvT te schrappen die erop kunnen duiden dat veilig inloggen zou mogen worden omzeild ten behoeve van het gebruiksgemak.

2.2 Gebruik privé-telefoon

Ingeschrevenen kunnen naast een pas bijvoorbeeld ook kiezen voor een digitale wallet op een smartphone of tablet. Als daarvoor een werktelefoon wordt gebruikt, zijn daarop mogelijk al diverse beveiligings-maatregelen ingesteld. Uit navraag bij het ministerie blijkt echter dat ook de privételefoon gebruikt kan worden. Dat hoeft geen probleem te zijn, mits de juiste richtlijnen worden nageleefd om de risico's die met het gebruik daarvan kunnen ontstaan op te vangen. De controle op die naleving kan evenwel mogelijk lastiger blijken dan bij een werktelefoon, nu een werkgever niet zomaar mag monitoren welke andere apps

[36] MvT p. 24.

een werknemer op zijn telefoon installeert. Als één medewerker malware op diens telefoon installeert, wat regelmatig gebeurt bij privételefoons,[37] zou dat al kunnen leiden tot een inbreuk van het zorgsysteem.

De AP adviseert in de MvT, waar het gaat om het gebruik van mobiele apparaten, ook toe te lichten welke risico's bestaan bij het gebruik van privételefoons en hoe die risico's kunnen worden ondervangen. Deze risico's en de beveiligingsmaatregelen daartegen zouden naar het oordeel van de AP ook moeten worden meegewogen bij de ontwikkeling en goedkeuring van nieuwe inlogmiddelen.

3. Registratie zorgmedewerkers

Naast zorgaanbieders, indicatieorganen en zorgverzekeraars kunnen op grond van het nieuwe artikel 14, eerste lid, aanhef, van het concept nu ook zorgmedewerkers zich registreren in het UZI-register. Die groep natuurlijke personen is breder dan de groep die ook onder het zorgaanbiedersbegrip uit artikel 1 Wet kwaliteit, klachten en geschillen zorg (Wkkgz) valt: "*een instelling dan wel een solistisch werkende zorgverlener*". Onder het nieuwe begrip zorgmedewerkers vallen namelijk niet alleen zorgverleners, maar bijvoorbeeld ook administratieve medewerkers, studenten, stagairs of leidinggevenden. Kortgezegd, iedereen die in de zorgsector werkt of wil werken. Uit navraag bij het ministerie blijkt dat daarop niet wordt gecontroleerd: "*Voor natuurlijke personen (zorgmedewerkers, niet zijnde zorgaanbieders) zijn er geen weigeringsgronden. Een intrekking van een inschrijving in het register is* [wel] *mogelijk.*" Het gevolg daarvan is dat onbegrensd is wie zich kan registreren in het UZI-register. Ook al is inschrijving zonder autorisatie door een aangesloten instelling in principe nutteloos, het opent mogelijk wel een deur voor misbruik. Dat kan worden voorkomen door te vereisen dat iemand moet aantonen werkzaam te zijn in de zorgsector, of dat binnen afzienbare tijd te zullen zijn. Bijvoorbeeld door te vereisen dat iemand een e-mailadres opgeeft met een domeinnaam van een bij het register aangesloten instelling.

De AP adviseert om het register zo in te richten dat alleen natuurlijke personen die aantoonbaar werkzaam zijn in de zorgsector, of dat binnen afzienbare tijd zullen zijn, kunnen worden ingeschreven.

4. Aangesloten diensten

4.1 Diensten anders dan EUS of zorginformatiesystemen

Uit het concept blijkt dat ingeschrevenen met een goedgekeurd inlogmiddel toegang kunnen krijgen tot SBV-Z, elektronische uitwisselingssystemen en zorginformatiesystemen.[38] Gelet op hetgeen vermeld staat op p. 2 van dit advies en voetnoot 7 zijn er echter ook andere diensten waarop zal kunnen worden ingelogd met een goedgekeurd inlogmiddel. Een voorbeeld is het Landelijk Implantatenregister. Dat register wordt in stand gehouden door de minister van VWS en is er voor bedoeld dat de Inspectie Gezondheidszorg en Jeugd (IGJ) naar aanleiding van een signaal over een veiligheidsrisico rond een bepaald implantaat zorgaanbieders kan informeren over de problemen met dat implantaat.[39] Dat register valt dus niet onder

[37] Zie bv: Politie en Fraudehelpdesk druk met Android-malware: 'Dit is iets nieuws, iets anders' (nos.nl) en Duizenden Nederlanders hebben malware op hun mobiel na valse sms over pakketje (nos.nl).
[38] Artikel 14, eerste lid onder a en b en artikel 14a, tweede lid.
[39] Factsheet 'Landelijk Implantatenregister voor zorgverleners en –aanbieders' van het ministerie van VWS.

de definitie in de Wabvpz van een elektronisch uitwisselingssysteem, waarvoor uitwisseling van zorgaanbieders aan andere zorgaanbieders vereist is, noch onder die van een zorginformatiesysteem.

De AP adviseert een aanvullende grondslag op te nemen voor het gebruik van de nieuwe inlogmiddelen voor de categorieën van diensten die nu buiten de boot vallen.

4.2 HR-systemen

Het wordt blijkens de MvT "*mogelijk gemaakt om een koppeling met een HR-systeem te maken voor geautomatiseerd aanmelden in het register*".[40] De achtergrond hiervan is, zo blijkt uit navraag bij het ministerie, dat grote zorginstellingen met veel zorgmedewerkers veel tijd kwijt zullen zijn met het handmatig doorgeven van initiële inschrijvingen en mutaties. Met een koppeling tussen het HR-systeem van de zorgaanbieder en het UZI-register worden in- en uitdiensttredingen onmiddellijk doorgegeven zodat ongeoorloofde toegang wordt bemoeilijkt.

De AP adviseert deze toelichting ook op te nemen in de MvT. Daarnaast adviseert de AP om in te gaan op de beveiligingsrisico's die gepaard kunnen gaan met een dergelijke koppeling, en op de eisen waaraan zulke HR-systemen moeten voldoen.

5. Overig

5.1 Te grote nadruk op gegevensuitwisseling

In artikel 14, eerste lid, onder b van het concept wordt gesproken van 'elektronische gegevensuitwisseling'. Ook in de MvT ligt de nadruk vaak op de uitwisseling van gegevens,[41] terwijl het net zo goed, misschien zelfs vaker, gaat over toegang tot de eigen zorginformatiesystemen.

De AP adviseert om artikel 14, eerste lid, onder b, van het concept zo aan te passen dat, overeenkomstig artikel 14a, tweede lid, van het concept niet alleen wordt gesproken van 'elektronische gegevensuitwisseling in de zorg', maar ook van 'toegang tot zorginformatiesystemen'.

5.2 Verruiming bevoegdheden IGJ

In het concept worden de nieuwe artikelen 14 en 15 Wabvpz geschaard onder de reikwijdte van de toezichts- en handhavingsbevoegdheden die in het wetsvoorstel Verzamelwet Gegevensverwerking VWS II aan de IGJ zijn toebedeeld. De AP heeft in haar advies op dat eerdere wetsvoorstel geadviseerd om beter te onderbouwen waarom het huidige instrumentarium van de AP en de IGJ niet voldoende is om de handhaafbaarheid van de Wabvpz te waarborgen.[42]

De AP adviseert in dit concept rekening te houden met de uitvoering van het eerdere advies van de AP.

[40] MvT p. 25.
[41] Zie meerdere voorbeelden op MvT p. 1 en p. 2.
[42] Advies AP van 17 oktober 2023 over de 'Verzamelwet Gegevensverwerking VWS II' (z2023-00615), onderdeel 13.

Datum
28 november 2023

Ons kenmerk
z2023-02938

Werklast AP

De AP merkt op dat het concept naar verwachting niet zal nopen tot extra inzet door de AP.

Openbaarmaking

Dit advies wordt binnen twee weken op de website van de AP gepubliceerd.

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter