Ministerie van Volksgezondheid,
Welzijn en Sport

Regeling van de Minister van Volksgezondheid,
Welzijn en Sport van
houdende wijziging van de Uitvoeringsregeling Wkkgz in
verband met de beveiliging van gegevens en de wijze van
pseudonimisering ten behoeve van registraties ter
bevordering van de kwaliteit en veiligheid van de
gezondheidszorg

De Minister van Volksgezondheid, Welzijn en Sport,

Gelet op de artikelen 4.4, onderdelen a en b, en 4.8, onderdelen a en b, van het Uitvoeringsbesluit Wkkgz;

Besluit:

Artikel I

De Uitvoeringsregeling Wkkgz wordt als volgt gewijzigd:

A

In artikel 1 worden in de alfabetische rangschikking de volgende begripsomschrijvingen ingevoegd:

Algemene verordening gegevensbescherming: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (PbEU 2016, 119);
NEN: door de Stichting Nederlands Normalisatie-instituut uitgegeven norm;
NEN 7510-1 en 7510-2: NEN 7510-1 en 7510-2 betreffende het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg;
NEN 7524:2019 en: NEN 7524:2019 en betreffende de pseudonimisering van gegevens in de zorg.

B

Na artikel 7 wordt een nieuw hoofdstuk ingevoegd:

Hoofdstuk 2A. Kwaliteitsregistraties

Artikel 7a

Aan artikel 5, eerste lid, onderdeel f, van de Algemene Verordening gegevensbescherming wordt in elk geval voldaan als de gegevens, bedoeld in de artikelen 4.2 en 4.6 van het Uitvoeringsbesluit Wkkgz, overeenkomstig NEN 7510-1 en NEN 7510-2, dan wel op een vergelijkbare wijze worden verstrekt en verwerkt.

Artikel 7b

Voor de uitvoering van deze regeling wordt toepassing gegeven aan de laatste uitgave van de NEN 7510-1 en NEN 7510-2. De minister doet van een nieuwe uitgave van de genoemde NEN, mededeling in de Staatscourant. Bij die mededeling wordt bekend gemaakt op welke datum de nieuwe uitgave van toepassing wordt.

Artikel 7c

De pseudonimisering, bedoeld in de artikelen 30a, derde lid, en 30b, vierde lid, van de wet, vindt zodanig plaats dat herleidbaarheid naar de persoon aan wie de gegevens toebehoren zo veel als mogelijk wordt voorkomen.

Artikel 7d

Aan artikel 7c wordt in elk geval voldaan als de pseudonimisatie plaatsvindt overeenkomstig NEN 7524:2019 en, dan wel op een vergelijkbare wijze.

Artikel II

Deze regeling treedt in werking met ingang van 1 juli 2022.

De Minister van Volksgezondheid,
Welzijn en Sport,

E.J. Kuipers

Toelichting

1. Algemeen

Deze ministeriële regeling wijzigt de Uitvoeringsregeling Wkkgz en is de uitwerking bij ministeriële regeling van hetgeen is bepaald in de artikelen 30a, vierde lid, onderdelen b en c, en 30b, zesde lid, onderdelen b en c, van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en de artikelen 4.4 en 4.8 van het Uitvoeringsbesluit Wkkgz.

De reden voor de wijziging van de Wkkgz, het invoegen van de nieuwe artikelen 30a en 30b[1], is het opnemen van een verwerkingsgrondslag voor persoonsgegevens, waaronder gezondheidsgegevens, ten behoeve van de kwaliteitsregistraties Landelijk Alcohol en Drugs Informatie Systeem (LADIS) met gegevens over verslaving(szorg) en de Landelijke Trauma Registratie (LTR) met gegevens over traumazorg per regio en op landelijk niveau. Ook is met deze artikelen geregeld dat zorgaanbieders die verslavingszorg verlenen en zorgaanbieders die acute zorg verlenen verplicht zijn alle noodzakelijke (persoons)gegevens, waaronder gegevens over de gezondheid, voor de in de artikelen 30a en 30b opgenomen doelen te verstrekken.

Gelet op de artikelen 30a, derde lid, en 30b, vierde lid, van de Wkkgz mogen de verwerker van LTR en de verwerker van LADIS de persoonsgegevens slechts verwerken als deze gepseudonimiseerd zijn. Dit houdt in dat de verwerkers van LADIS en LTR ervoor verantwoordelijk zijn dat de persoonsgegevens worden gepseudonimiseerd.

Pseudonimisering van persoonsgegevens houdt in dat deze gegevens op zodanige wijze zijn verwerkt dat ze niet zonder het gebruik van aanvullende gegevens herleidbaar zijn tot specifieke natuurlijke personen. Dit betekent dat bij persoonsgegevens het persoonsidentificerende gedeelte (bijvoorbeeld naam, adres en woonplaats of het Burgerservicenummer (hierna: BSN) is versleuteld tot fictieve nummers, letters of andere symbolen. De betrokkene wordt vervolgens met die fictieve nummers, die letters of die symbolen aangeduid. Uit de begripsomschrijving "pseudonimisering" in artikel 4, onderdeel 5, van de AVG blijkt dat een dergelijke bewerking van persoonsgegevens als een verwerking van persoonsgegevens in de zin van die verordening geldt. De pseudonimisering van persoonsgegevens vormt een methode om de inbreuk op de bescherming van persoonsgegevens als gevolg van de verwerking zoveel mogelijk te beperken. De pseudonimisering mag ook niet ongedaan zijn gemaakt, maar moet onafgebroken worden gecontinueerd.

In de artikelen 30a en 30b van de Wkkgz is een delegatiegrondslag opgenomen voor het bepalen van de wijze van verstrekking en verwerking van gegevens. Dit gaat onder meer over de wijze van pseudonimiseren. Ook moet de wijze waarop persoonsgegevens, waaronder gezondheidsgegevens, door passende technische en organisatorische maatregelen worden beveiligd tegen verlies of onrechtmatige verwerking, worden opgenomen in lagere regelgeving. In de artikelen 4.4 en 4.8

[1] Stb. 2021, 496

van het Uitvoeringsbesluit Wkkgz zijn deze twee onderwerpen doorgedelegeerd naar het niveau van een ministeriële regeling.

2. Vereisten beveiliging van gegevens AVG

Artikel 5, eerste lid, onderdeel f, van de AVG bepaalt dat bij de verwerking van persoonsgegevens passende en organisatorische maatregelen moeten worden getroffen, zodat een passende beveiliging is gewaarborgd en dat persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking. Op grond van artikel 32, eerste lid, van de AVG zijn zowel de verwerkingsverantwoordelijke als de verwerker verplicht passende technische en organisatorische maatregelen te treffen. Vervolgens is bepaald wat kan worden verstaan onder passende en organisatorische maatregelen. Eén van deze maatregelen is pseudonimisering en versleuteling van persoonsgegevens[2]. Uit het vorenstaande blijkt dat deze waarborg is getroffen aangezien de verwerkers van LADIS en LTR de persoonsgegevens slechts mogen verwerken als deze gepseudonimiseerd zijn.

In deze regeling wordt geen bepaalde wijze van pseudonimiseren verplicht gesteld. Wel wordt bepaald dat aan een rechtmatige verwerking van de persoonsgegevens wordt voldaan als wordt gepseudonimiseerd conform NEN 7524:2019 en (hierna: NEN 7524) of op een vergelijkbare wijze. Ook wordt in deze regeling geen bepaalde wijze van beveiliging vastgelegd. De beveiliging van persoonsgegevens tegen verlies en onrechtmatige verwerking, welk vereiste is opgenomen in artikel 5, eerste lid, onderdeel f, van de AVG, is in elk geval geborgd als wordt voldaan aan NEN 7510-1:2017+A1:2020 nl (hierna: NEN 7510-1) en NEN 7510-2:2017 (hierna: NEN 7510-2) dan wel als de beveiliging plaatsvindt op een vergelijkbare wijze.

3. NEN-normen

Als er sprake is van zelfregulering, kan in een regeling worden verwezen naar een norm die niet publiekrechtelijk van aard is. Dit kunnen bijvoorbeeld normalisatienormen zijn. Van normalisatie is sprake als private partijen door tussenkomst van bijvoorbeeld het Nederlands Normalisatie-instituut NEN gezamenlijk normen voor hun handelen opstellen.

3.1. Informatiebeveiliging NEN 7510-1 en NEN 7510-2

Voor de informatiebeveiliging in de zorg zijn NEN-normen beschikbaar. Dit zijn onder meer de NEN 7510-1 en NEN 7510-2.

Binnen de Nederlandse Zorg zijn NEN 7510-1 en NEN 7510-2 dé normen als het gaat om informatiebeveiliging. Deze normen dekken het hele gebied van informatiebeveiliging, zowel op technisch, als organisatorisch en procedureel niveau. NEN 7510-1 en NEN 7510-2 geven richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie moeten treffen ter beveiliging van de informatievoorziening. Het ministerie van VWS eist van instellingen in de gezondheidszorg dat de informatiebeveiliging op orde is. De NEN 7510-1 en NEN

[2] Artikel 32, eerste lid, onderdeel a, van de AVG

7510-2 worden daarbij als kader gehanteerd. Het ministerie van VWS heeft een overeenkomst met NEN gesloten over de afkoop van onder andere de NEN 7510 (later NEN 7510-1 en 7510-2) per 1 november 2014, waardoor NEN 7510-1 en 7510-2 voor een ieder kosteloos digitaal beschikbaar zijn.

De primaire doelgroep van NEN 7510-1 en 7510-2 is de zorginstelling. Toeleveranciers van de zorg, bijvoorbeeld organisaties die patiënten informatie verwerken, maken in de praktijk echter ook gebruik van deze NEN normen.

Certificering op grond van NEN 7510-1 en 7510-2 wordt in deze regeling niet verplicht gesteld. Hetzelfde resultaat kan ook op een andere wijze worden bereikt. Dit is conform het uitgangspunt dat bij het gebruik van normen in beleid of wetgeving de toepassing van normen vrijwillig is. Er wordt gericht op een niet-dwingende wijze van verwijzen. Dit blijkt uit het kabinetsbeleid inzake de kenbaarheid van normen en normalisatie (hierna: kabinetsbeleid normen en normalisatie).[3] De reden dat het dwingend opleggen van bijvoorbeeld NEN-normen minder wenselijk is dat op deze normen een auteursrecht rust en alleen tegen betaling kunnen worden verkregen. Daarbij komt dat normalisatie een vrijwillig karakter kent en om die reden niet goed valt te rijmen met het dwingend opleggen van deze normen. Echter, in sommige gevallen wordt een NEN-norm toch dwingend opgelegd. In dat geval is het uitgangspunt conform het kabinetsbeleid normen en normalisatie dat de overheid de norm afkoopt, zodat deze voor een ieder kosteloos toegankelijk is.

In deze regeling wordt verwezen naar artikel 5, eerste lid, onderdeel f, van de AVG, omdat daarin wordt bepaald dat bij het verwerken van persoonsgegevens, waarvan sprake is bij gepseudonimiseerde persoonsgegevens, voor een afdoende beveiligingsniveau moet worden zorg gedragen. In artikel 7a is bepaald dat hier in elk geval aan wordt voldaan als de gegevens worden verwerkt conform de NEN 7510-1 en 7510-2 dan wel op een vergelijkbare wijze worden verwerkt. Hoewel NEN 7510-1 en 7510-2 zijn afgekocht en het om die reden ook mogelijk is om deze verplicht op te leggen, is hier gelet op het vorenstaande niet voor gekozen.

In andere gevallen worden NEN 7510-1 en 7510-2 wel dwingend voorgeschreven. Zo zijn zorgaanbieders bijvoorbeeld op grond van artikel 2 van de Regeling gebruik Burgerservicenummer in de zorg wel verplicht te voldoen aan de NEN 7510-1 en 7510-2 als zij het burgerservicenummer verwerken.

3.2 Pseudonimisering NEN 7524

Pseudonomiseren op grond van NEN 7524 wordt in deze regeling niet verplicht gesteld. Hetzelfde resultaat kan ook op een andere wijze worden bereikt. Voor de dienstverlening ten aanzien van pseudonimisering heeft NEN in juli 2019 de Nederlandse norm NEN 7524 gepubliceerd. De NEN 7524 is opgesteld door gebruikers en leveranciers van pseudonimisatiediensten. Het doel van de norm NEN 7524 is de privacy van de patiënten te respecteren en de beschikbaarheid van de gegevens over langere tijd veilig te stellen. De NEN 7524 ziet zowel op het verschaffen van zekerheid over de wijze waarop een pseudonimiseringsdienst wordt verleend, als op de kwaliteit waarmee dat gedaan wordt.

[3] Kamerstukken II, 2010/11, 27406, nr. 193

De NEN 7524 is een Nederlandse variant als aanvulling op de internationale norm ISO 25237, waarin de verschillende vormen van pseudonimisering staan opgesomd.

In artikel 7c van deze regeling is de norm neergelegd dat met het pseudonimiseren van de gegevens zoveel mogelijk moet worden voorkomen dat de gegevens herleidbaar zijn naar de persoon aan wie ze toebehoren. Met het pseudonimiseren is herleidbaarheid naar de persoon niet uit te sluiten, maar wel kan met de juiste wijze van pseudonimiseren herleidbaarheid zoveel mogelijk worden voorkomen. Aan de in artikel 7c neergelegde norm wordt in elk geval voldaan als wordt gehandeld in overeenstemming met NEN 7524 dan wel een vergelijkbare wijze van pseudonimisering wordt gehanteerd. Kortom, in deze regeling wordt verwezen naar de NEN 7524, maar de norm niet is verplichtend opgelegd. Dit is in lijn met het voorgaande.

3.3. De betrokken verwerkingsverantwoordelijke en verwerkers

3.3.1 LADIS

In onderstaande tabel zijn de partijen die betrokken zijn bij de gegevensverwerking van de persoonsgegevens in LADIS weergegeven. Dit zijn de verstrekkers van de gegevens aan LADIS (de Nederlandse zorgaanbieders die verslavingszorg bieden en apothekers die opiaatvervangende middelen registreren die zij verstrekken ten behoeve van een opiaatonderhoudsbehandeling in de verslavingszorg), de verwerker van LADIS (IVZ) en de sub verwerker (ZorgTTP). Deze partijen moeten veiligheidseisen treffen en ervoor zorgdragen dat de pseudonimisering zodanig wordt vormgegeven dat zo veel mogelijk wordt voorkomen dat de gegevens niet meer zijn terug te leiden naar de persoon aan wie ze toebehoren.

Organisatie	Rol				Toegang vanuit LADIS database	
	Verantwoor-delijke	Verstrekker	Verwerker	Ontvanger	Functionaris	Gegevens
Ministerie van VWS	X			X	Minister	Toegang tot geaggregeerde rapportages
Stichting IVZ			X		Data management medewerkers	Toegang tot alle gegevens vastgelegd in LADIS na tweede versleuteling en geaggregeerde rapportages
ZorgTTP			X		Operationeel managers	Toegang tot alle gegevens aangeleverd door zorgaanbieders na eerste versleuteling. De aan de bron versleutelde gegevens worden in een geautomatiseerd proces in een beveiligde omgeving verwerkt en na tweede versleuteling beschikbaar gesteld voor IVZ
Verslavings-zorginstellingen		X		X	Data management medewerkers	Toegang tot alle gegevens van cliënten in de verslavingszorg en geaggregeerde rapportages na verwerking in LADIS.

Tabel 1. Schematische weergave van de organisaties betrokken bij de gegevensverwerking in LADIS en de mate waarin zij toegang hebben tot de gegevens.

Nadere toelichting is te vinden in paragraaf 2 van de nota van toelichting bij wijziging van het Uitvoeringsbesluit Wkkgz waar[4] is beschreven op welke wijze de datastroom vanuit de zorginstelling via verwerker ZorgTTP naar de verwerker van LADIS plaatsvindt.

Artikelen 7a en 7c van deze regeling zijn op deze partijen van toepassing, inhoudende dat de verstrekking en verwerking van de gegevens geschiedt overeenkomstig NEN 7510-1, NEN 7510-2 en (in geval van pseudonimisering) NEN 7524 of op vergelijkbare wijze.

Voor de kwaliteitsregistratie LADIS verwerkt de minister gepseudonimiseerde persoonsgegevens voor de in artikel 30a, eerste lid, van de wet genoemde doeleinden. De minister is de verwerkingsverantwoordelijke en maakt gebruik van een verwerker, die 7510-1 en 7510-2 NEN gecertificeerd is, en heeft hiervoor een verwerkingsovereenkomst gesloten. De verwerkers van LADIS en LTR zijn ervoor verantwoordelijk dat de gegevens worden gepseudonimiseerd.

[4] PM Staatsblad

3.3.2 LTR

In onderstaande tabel zijn de partijen die betrokken zijn bij de gegevensverwerking van de persoonsgegevens in LTR weergegeven. Dit zijn de verstrekkers van de gegevens aan LTR (ziekenhuizen met een afdeling spoedeisende hulp waar ongeval patiënten kunnen worden opgevangen en behandeld voor hun letsel en ambulancediensten die prehospitaal hulp verlenen aan ongevalpatiënten), de verwerkers van LTR (ADM LUMC en IVZ) en de sub verwerker (ZorgTTP). Deze partijen moeten veiligheidseisen treffen en ervoor zorgdragen dat de pseudonimisering zodanig wordt vormgegeven dat zo veel mogelijk wordt vooromen dat de gegevens niet meer zijn terug te leiden naar de persoon aan wie ze toebehoren.

Organisatie	**Rol**				**Toegang vanuit LTR database**	
	Verantwoor-delijke	Verstrekker	Verwerker	Ontvanger	Functionaris	Gegevens
Ambulancedienst		X			Medewerker ambulance-dienst	Toegang tot alle gegevens van ongevalpatiënten vastgelegd in de LTR aangeleverd door de ambulancedienst.
Ziekenhuis afdeling SEH		X			Medewerker ziekenhuis	Toegang tot alle gegevens van ongevalpatiënten vastgelegd in de LTR aangeleverd door het ziekenhuis.
Aangewezen traumacentrum	X			X	Datamanager regionale trauma-registratie Medewerker landelijke trauma-registratie	Toegang tot alle gepseudonimiseerde en overige gegevens van ongevalpatiënten vastgelegd in de LTR door de ambulancediensten en ziekenhuizen binnen het traumanetwerk van het betreffende traumacentrum.
ADM LUMC			X	X	Data management medewerkers	Toegang tot de gepseudonimiseerde en overige gegevens van ongevalpatiënten vastgelegd in de LTR.
IVZ			X	X	Medewerker	Toegang tot set gepseudonimiseerde en overige gegevens van alle ongevalpatiënten vastgelegd in de LTR benodigd voor de vastgestelde terugkoppelrapportages.

Tabel 2. Schematische weergave van de organisaties betrokken bij de gegevensverwerking in de LTR en de mate waarin zij toegang hebben tot de gegevens.

Nadere toelichting is te vinden in paragraaf 3 van de nota van toelichting bij wijziging van het Uitvoeringsbesluit waar [5] tevens is beschreven op welke wijze de datastroom vanuit de zorginstelling via verwerker ZorgTTP naar de verwerker van LTR plaatsvindt.

Artikelen 7a en 7c van deze regeling zijn op deze partijen van toepassing, inhoudende dat de verstrekking en verwerking van de gegevens geschiedt overeenkomstig NEN 7510-1, NEN 7510-2 en (in geval van pseudonimisering) NEN 7524 of op vergelijkbare wijze.

3.4 Dynamische en statische verwijzing

In het geval in een regeling wordt verwezen naar niet publiekrechtelijke normen, zoals in deze regeling, is het uitgangspunt dat naar deze normen statisch wordt verwezen. Dit betekent dat wordt verwezen naar normen zoals deze op een bepaald tijdstip moment luiden.

Conform dit uitgangspunt wordt in de regeling naar NEN 7524 statisch verwezen. In de regeling is dit ook terug te zien doordat in de begripsbepaling de versie van NEN 7524 is opgenomen.

Ondanks het voorgaande is voor de NEN 7510-1 en 7510-2 gekozen voor een dynamische verwijzing. Bij toepassing van de normen, wordt dan steeds toepassing gegeven aan de laatste versie van de betreffende norm. In dat geval moet in de Staatscourant mededeling worden gedaan van wijzigingen in de norm. In de artikelen van deze regeling wordt dan ook verwezen naar NEN 7510-1 en 7510-2 zonder dat daarbij wordt genoemd welke versie het betreft. Voorts is in artikel 7d bepaald dat steeds toepassing dient te worden gegeven aan de laatst gepubliceerde versie en dat in de Staatscourant wordt gepubliceerd als sprake is van een nieuwe versie van de NEN 7510-1 en 7510-2. Ook wordt in de Staatscourant gepubliceerd op welk moment de nieuwe versie van kracht is. Eerder in deze toelichting is aangegeven welke versies van NEN 7510- en 7510-2, op het moment dat deze regeling in werking is getreden, van toepassing zijn. De reden dat is gekozen voor een dynamische verwijzing is dat reeds op grond van artikel 7 van het Besluit elektronische gegevensverwerking door zorgaanbieders sprake is van een dynamische verwijzing van NEN 7510 (eerdere versie van de NEN 7510-1 en 7510:2). Als er sprake is van een nieuwe versie van NEN 7510-1 en 7510-2, wordt dit reeds gepubliceerd op grond van artikel 7 van dit besluit. Om die reden wordt hierbij aangesloten en is in dit geval niet gekozen voor een statische verwijzing.

4. Gevolgen van de regelgeving voor de regeldruk

De in deze regeling gestelde regels over de beveiliging en de wijze van pseudonimiseren van persoonsgegevens komen overeen met de staande praktijk en leiden derhalve niet tot een verzwaring van de regeldruk voor de partijen op wie deze regels van toepassing zijn.
PM ATR

[5] PM Staatsblad

De Minister van Volksgezondheid,
Welzijn en Sport,

E.J. Kuipers