Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

22 112 **Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie**

27 529 **Informatie- en Communicatietechnologie (ICT) in de Zorg**

Nr. 3785

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 oktober 2023

Met deze brief informeer ik uw Kamer over de waarborgen binnen het Commissievoorstel voor een European Health Data Space (hierna: EHDS-voorstel). Het voorstel beoogt elektronische gezondheidsgegevens zo veilig mogelijk beschikbaar te stellen voor primair en secundair gebruik. Hierbij kom ik tegemoet aan mijn toezegging van 1 juni 2023, tijdens het tweeminutendebat naar aanleiding van de EU-Gezondheidsraad (Handelingen II 2022/23, nr. 88, item 10). Voor deze toelichting op de waarborgen ga ik uit van het EHDS-voorstel dat op 3 mei 2022 is gepubliceerd. Op dit moment bevindt het EHDS-voorstel zich nog in de onderhandelingsfase in zowel de Raad als het Europees Parlement. Om die reden worden er door beide instituten afzonderlijk nog inhoudelijke aanpassingen gemaakt voordat zij tot een eigen compromistekst komen. Pas daarna kunnen de interinstitutionele onderhandelingen tussen de Raad, het Europees Parlement en de Europese Commissie (de triloog) beginnen. Hoewel ik uitga van het Commissievoorstel, neem ik in deze brief ook relevante ontwikkelingen uit de onderhandelingen in de Raad mee.

1. Doelstellingen van het EHDS-voorstel

Het EHDS-voorstel heeft drie doelstellingen:
1. het verbeteren van de toegang voor burgers tot persoonlijke elektronische gezondheidsgegevens en zeggenschap daarover in de context van de zorgverlening *(primair gebruik)*;
2. het bieden van een uniform juridisch kader voor de ontwikkeling, het in de handel brengen en het gebruik van elektronisch patiëntendossier systemen (hierna: EPD-systemen);
3. het vergemakkelijken van het (her)gebruik van elektronische gezondheidsgegevens voor andere doeleinden, zoals wetenschappelijk onderzoek, innovatie en beleidsvorming *(secundair gebruik)*.

kst-22112-3785
ISSN 0921 - 7371
's-Gravenhage 2023

Het EHDS-voorstel omvat regels die gezondheidsgegevens in de Europese Unie (hierna: EU) veilig en verantwoord breder beschikbaar moeten maken. Dit om burgers overal in de EU betere en snellere zorg te kunnen bieden. Daarnaast is het uitgangspunt dat er op grotere schaal onderzoek kan plaatsvinden, innovaties worden ontwikkeld en beleid kan worden geëvalueerd en verbeterd. Dit alles moet bijdragen aan de volksgezondheid en welzijn.

2. Verhouding met nationaal beleid

Het uitgangspunt van het EHDS-voorstel voor betere beschikbaarheid van gezondheidsgegevens (databeschikbaarheid) sluit aan op en geeft op sommige aspecten invulling aan, het nationale beleid zoals is verwoord in de *Nationale Visie op het Gezondheidsinformatiestelsel*[1] en de *Visie en strategie op secundair datagebruik*[2]. Verbetering van databeschikbaarheid is ook wat de Wet elektronische gegevensuitwisseling in de zorg (hierna: Wegiz)[3] nastreeft. Hiermee verbeteren wij de kwaliteit van zorg en kunnen wij de administratieve lasten verminderen. Databeschikbaarheid draagt daarmee bij aan een toekomstbestendige zorg.

Zoals in de Nationale Visie op het Gezondheidsinformatiestelsel is aangegeven, is voor goede databeschikbaarheid het vertrouwen van de burger in integere omgang met deze gegevens randvoorwaardelijk. Ook in het EHDS-voorstel wordt dit onderkend. Het EHDS-voorstel omvat waarborgen die ervoor moeten zorgen dat veilig en verantwoord met gezondheidsgegevens wordt omgegaan.

Over de verhouding tussen het EHDS-voorstel en het nationaal zorginformatiebeleid heb ik uw Kamer uitgebreider geïnformeerd in mijn vorige brieven over de voortgang van de EHDS en de uitgevoerde impactanalyses.[4] Voor een algemeen overzicht van de Nederlandse inzet in de onderhandelingen verwijs ik u naar het BNC-fiche dat ik in juni 2022 met u heb gedeeld.[5]

3. Verhouding met privacy en gegevensbescherming

Zoals gezegd kan databeschikbaarheid niet zonder vertrouwen. Als burgers niet het vertrouwen hebben dat hun gegevens veilig zijn bij de zorgverlener, kunnen zij zorg gaan mijden of minder informatie met de zorgverlener delen. En wanneer burgers geen zeggenschap hebben over wie welke informatie krijgt, wordt de privacy beperkt.

Het recht op bescherming van de persoonlijke levenssfeer (privacy) van burgers en op bescherming van persoonsgegevens worden door internationale verdragen, zoals het Europees Verdrag voor de Rechten van de Mens, het EU-Handvest van de grondrechten en de Europese Algemene Verordening Gegevensbescherming (hierna: AVG) gewaarborgd.

Bij de ontwikkeling van het EHDS-voorstel is het uitgangspunt dat de EHDS niet in strijd mag zijn met de hiervoor genoemde Europese verdragen en de AVG. Voor de AVG betekent dit dat de daarin bepaalde waarborgen en beginselen onverkort blijven gelden. Zo bepaalt de AVG dat verwerking van persoonsgegevens altijd rechtmatig, behoorlijk en

---

[1] Kamerstuk 27 529, nr. 292.
[2] Kamerstuk 27 529, nr. 294.
[3] Kamerstuk 35 824, nr. 2.
[4] Kamerstukken 22 112 en 27 529, nr. 3604; Kamerstukken 27 529 en 35 824, nr. 285.
[5] Kamerstuk 22 112, nr. 3458.

transparant moet zijn en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Het EHDS-voorstel geeft invulling aan de ruimte die de AVG biedt om op bepaalde onderwerpen nadere Europese wetgeving tot stand te brengen die voorziet in grondslagen voor de verwerking en uitwisseling van (bijzondere) persoonsgegevens. Het EHDS-voorstel voorziet in lijn met de AVG in juridische grondslagen, zodat voor primair en secundair gebruik gezondheidsgegevens kunnen worden verwerkt zonder toestemming van de persoon van wie de gegevens worden gebruikt. Dit komt de databeschikbaarheid ten goede. De EHDS gaat daarmee uit van een andere AVG-grondslag dan de huidige Nederlandse wetgeving. Op dit moment wordt in Nederland als juridische grondslag voor het verwerken van gezondheidsgegevens hoofdzakelijk toestemming gebruikt. Om de privacy en de vrije toegang tot de zorg te borgen bevat het EHDS-voorstel daarbij (privacy) waarborgen die ervoor moeten zorgen dat veilig en verantwoord met gezondheidsgegevens wordt omgegaan. Hierna zal ik verder ingaan op de waarborgen die in het EHDS-voorstel specifiek voor primair en secundair gegevensgebruik zijn opgenomen, in aanvulling op de waarborgen die al in de AVG staan.

4. Waarborgen bij primair gebruik van elektronische gezondheidsgegevens

Bij primair gebruik gaat het om het gebruik van gezondheidsgegevens ten behoeve van het verlenen van zorg. Het EHDS-voorstel neemt voor primair gebruik als uitgangspunt dat zes prioritaire categorieën elektronische gezondheidsgegevens[6] uit EPD-systemen EU-breed toegankelijk moeten zijn voor zorgprofessionals en aanbieders, wanneer dit nodig is voor de verlening van zorg. Het begrip EPD omvat in het EHDS-voorstel meer dan enkel de EPD-systemen die gebruikt worden in de ziekenhuissector en de reikwijdte van zorgverlening waar de bepalingen voor primair gebruik van toepassing zijn staat nog ter discussie. Om die toegankelijkheid te realiseren bevat het EHDS-voorstel een regeling die met zich meebrengt dat die prioritaire gegevens uit het EPD in beginsel toegankelijk zijn, zonder dat de burger onder behandeling (de cliënt) daarvoor voorafgaand toestemming moet geven. Lidstaten mogen naast de vereiste prioritaire categorieën van EHDS-voorstel ook zelf de hoeveelheid gegevens uitbreiden. Momenteel staat het mandaat van de Europese Commissie om de lijst prioritaire categorieën uit te breiden nog ter discussie.

Het EHDS-voorstel regelt niet dat op een centrale plaats in Europa persoonsgebonden gezondheidsgegevens worden verzameld. Het EHDS-voorstel creëert dus geen Europees EPD.

Rechten van burgers en regie van de burger op de toegang

Het EHDS-voorstel beoogt een centrale rol voor burgers ten aanzien van regie op de eigen elektronische gezondheidsgegevens voor primair gebruik. De burger krijgt in het voorstel specifieke rechten en lidstaten worden verplicht om deze te faciliteren via nationaal op te zetten toegangsdiensten.[7] Dit moet burgers meer grip geven op de toegang tot de elektronische gezondheidsgegevens door zorgprofessionals of

---

[6] De prioritaire gegevens betreffen: de patiëntsamenvatting, elektronische recepten, elektronische verstrekkingen, medisch beelden en bijbehorende verslagen, laboratoriumresultaten en bijbehorende rapporten en ontslagverslagen.

[7] In het EHDS-voorstel wordt gesproken over «een onlinedienst, zoals een portaal of een mobiele applicatie».

zorgaanbieders. Deze rechten worden als een belangrijke waarborg voor de privacy en vrije toegang tot de zorg gezien.

Zo krijgen burgers het recht de eigen gegevens en informatie over verwerking kosteloos en direct tot hun beschikking te krijgen via de toegangsdienst(en). Er dient volledige transparantie te zijn over welke zorgprofessional of -aanbieder toegang heeft gekregen tot de gegevens.

Daarnaast krijgen burgers het recht om de toegang door zorgprofessionals of -aanbieders tot alle of een deel van de gegevens in het EPD te beperken. De desbetreffende zorgprofessionals of -aanbieders hebben dan geen toegang tot de elektronische gezondheidsgegevens van de burger en de zorgaanbieder mag en kan die gegevens ook niet aan een andere zorgaanbieder verstrekken, tenzij het vitaal belang van de patiënt in het geding is. In de Raad vindt er momenteel een discussie plaats of aan burgers meer regie moet worden toegekend over de eigen gezondheidsgegevens, bijvoorbeeld door burgers meer rechten te geven om verwerkingen van gegevens tegen te houden. Zo ook specifieke beperkingen om elektronische gezondheidsgegevens op voorhand niet beschikbaar te stellen voor grensoverschrijdende uitwisseling via de daarvoor bestemde infrastructuur MyHealth@EU. Nederland vindt dit een belangrijk punt.[8]

Lidstaten bepalen zelf hoe zij de rechten voor burgers faciliteren en mogen passende keuzes maken bij hun nationale zorginformatiesysteem, zolang deze geen afbreuk doen aan de EHDS. Zo kunnen lidstaten zelf regels vaststellen voor de categorieën gezondheidsgegevens waartoe de verschillende beroepen in de gezondheidszorg (zorgverleners) toegang mogen krijgen.

Regels voor toegang door zorgprofessionals en -aanbieders

Zorgprofessionals en -aanbieders krijgen op basis van het EHDS-voorstel het recht op toegang tot elektronische gezondheidsgegevens over hun cliënten, ongeacht in welke lidstaat de zorgprofessional of -aanbieder is gesitueerd.

Zoals gezegd blijft de AVG volledig van toepassing. Dat betekent dat zorgprofessionals en -aanbieders zich niet alleen moeten houden aan de EHDS, maar ook de AVG. Zorgprofessionals en -aanbieders moeten dus altijd bevoegd zijn tot het inzien en verwerken van de desbetreffende gezondheidsgegevens, bijvoorbeeld omdat het verwerken van die gegevens nodig is voor een goede behandeling. EPD-systemen moeten de toegang tot de gegevens ondersteunen en elke verleende toegang bijhouden en loggen zodat burgers kunnen inzien wie er toegang tot hun EPD hebben gehad.

Hoe de hierboven genoemde toegang tot elektronische gezondheidsgegevens door zorgprofessionals en -aanbieders wordt gefaciliteerd dienen lidstaten zelf te bepalen. Hier hebben lidstaten zelf de keuze het te laten passen in het nationale zorginformatiesysteem, zolang dit geen afbreuk doet aan de EHDS.

Hierboven is al opgemerkt dat burgers het recht hebben om de toegang tot de gegevens te beperken. Als iemand dat recht heeft uitgeoefend, dan kan de zorgprofessional die gegevens niet inzien. Dit kan wel anders zijn als er sprake is van een vitaal belang. Als er een levensbedreigende situatie is, de gegevens noodzakelijk zijn om deze situatie te adresseren en

[8] Kamerstukken 22 112 en 27 529, nr. 3680.

de cliënt niet aanspreekbaar is om toestemming te geven voor de toegang tot de gegevens, kan de zorgprofessional toch de gegevens raadplegen *(breaking-the-glass)*. Daarbij geldt dat de cliënt altijd na afloop geïnformeerd moet worden door wie toegang is verkregen tot de gegevens. Transparantie is zoals genoemd een belangrijk uitgangspunt van het EHDS-voorstel (en de AVG) en wordt als belangrijke waarborg gezien voor privacy en vrije toegang tot de zorg. Als gegevens niet beschikbaar zouden zijn voor grensoverschrijdende uitwisseling via MyHealth@EU, dan is *breaking-the-glass* door zorgverleners of -aanbieders in andere lidstaten voor de desbetreffende gegevens niet mogelijk.

Decentrale digitale infrastructuur

De rechten en plichten die het EHDS-voorstel creëert gelden overal in de Europese Unie. Dit betekent dat de elektronische gezondheidsgegevens wanneer nodig in andere lidstaten toegankelijk zijn, met alle geldende beperkingen en waarborgen. Hiervoor is een grensoverschrijdende infrastructuur nodig. Momenteel werken de lidstaten hier samen aan met de Europese Commissie. Die digitale infrastructuur heet MyHealth@EU en is decentraal, bestaande uit een netwerk van nationale contactpunten voor eHealth (NCPeH's). De infrastructuur dient als een digitaal knooppunt voor de uitwisseling van gegevens tussen zorginformatiestelsels van lidstaten. Iedere lidstaat dient een NCPeH op te zetten conform technische, organisatorische en juridische vereisten. Daarop vindt een uitgebreide audit plaats voordat een NCPeH van een lidstaat wordt aangesloten op MyHealth@EU. Nederland heeft al een NCPeH opgezet dat sinds februari 2022 door het CIBG in is beheer genomen.[9]

Om de uitwisseling van de gegevens zo veilig mogelijk te laten plaatsvinden, is MyHealth@EU volledig losgekoppeld van het reguliere internet. Dit is gedaan ter voorkoming van cyberaanvallen van buitenaf. Daarnaast zijn de gegevens die worden uitgewisseld tussen de lidstaten volledig versleuteld door middel van end-to-end encryptie. Binnen MyHealth@EU is toegewerkt naar een infrastructuur waar geen sprake is van een zogenoemde *single-point-of-failure*. Indien er problemen worden ondervonden bij een NCPeH van een lidstaat, dan kan deze (tijdelijk) worden afgesloten van de gehele digitale infrastructuur zonder dat daarmee het hele systeem wordt stilgelegd. De uitwisseling van elektronische gezondheidsgegevens en daarmee de levering van de zorg kan hierdoor voor de resterende veilige NCPeH's worden gewaarborgd.

Vereisten aan EPD-systemen

EPD-systemen hebben een sleutelrol in het kunnen ontsluiten van de elektronische gezondheidsgegevens aan zorgprofessionals en -aanbieders.[10] Het EHDS-voorstel beoogt de interne markt voor EPD-systemen te reguleren. Bij de vereisten wordt de nadruk gelegd op het verzekeren van de hierboven genoemde waarborgen, bijvoorbeeld door eisen te stellen voor interoperabiliteit en veiligheid van EPD-systemen, waaronder *logging*. Het EHDS-voorstel beperkt zich tot EPD-systemen die ontwikkeld zijn voor het gebruik van de geprioriteerde categorieën elektronische gezondheidsgegevens uit het voorstel. Voor deze systemen gelden de vereisten van het EHDS-voorstel waaraan fabrikanten en leveranciers moeten voldoen. Het EHDS-voorstel beoogt dus op EPD-systeemniveau bepaalde essentiële waarborgen te garan-

[9] https://www.cibg.nl/actueel/nieuws/2022/02/09/het-nationaal-contactpunt-e-health-is-live

[10] De EPD-systemen in het EHDS-voorstel zijn zo gedefinieerd dat een elektronisch cliëntendossier (ECDs) daar ook onder valt. Hieronder vallen ook systemen die claimen gegevens te kunnen uitwisselen met EPD-systemen, zoals AI-systemen of medische hulpmiddelen.

deren waar de gebruiker van het systeem maar ook de burger wiens persoonlijke gezondheidsgegevens worden verwerkt op kan vertrouwen. Voor EPD-systemen gelden naast de vereisten uit het EHDS-voorstel straks ook de vereisten uit de Cyber Resilience Act verordening (CRA), zoals het vereiste om gegevens te versleutelen (bijvoorbeeld door end-to-end encryptie).[11] Op het CRA-voorstel is recentelijk een onderhandelingsmandaat namens de Raad vastgesteld.[12]

In het EHDS-voorstel wordt een systematiek voorgeschreven van zelfbeoordeling voordat een EPD-systeem wordt toegelaten tot de Europese interne markt. Dit houdt in dat de fabrikant zelf over interoperabiliteit en veiligheid oordeelt, de technische documentatie daarover opstelt en het product uiteindelijk voorziet van een CE-markering en conformiteitsverklaring. Er worden momenteel in de Raad gesprekken gevoerd om de conformiteitstoets door een onafhankelijke derde partij voorafgaand aan markttoelating te laten plaatsvinden. Ook dit is voor Nederland een belangrijk punt.

Toezichthoudende nationale digitale gezondheidsautoriteit (voor primair gebruik)

Om databeschikbaarheid op een verantwoorde, veilige en transparante wijze te stimuleren, moet iedere lidstaat een nationale digitale gezondheidsautoriteit aanwijzen. De nationale digitale gezondheidsautoriteit ziet toe op de naleving van rechten en plichten uit het EHDS-voorstel op het gebied van primair gebruik. Burgers kunnen bij deze autoriteit een klacht indienen wanneer hun rechten uit de EHDS worden geschonden. Bij schending van rechten en overtredingen kan de digitale gezondheidsautoriteit overgaan tot het treffen van maatregelen die voor de naleving moeten zorgen en in het uiterste geval kunnen sancties zoals boetes worden opgelegd. Gelet op de raakvlakken met het privacy- en gegevensbeschermingsrecht, gaat de Nederlandse digitale gezondheidsautoriteit nauw samenwerken met de Autoriteit Persoonsgegevens, die de verantwoordelijke toezichthouder blijft op naleving van de AVG.

5. Waarborgen bij secundair gebruik van elektronische gezondheidsgegevens

Waar het bij primair gebruik gaat om toegang tot gegevens in het kader van diagnostiek en behandeling van een specifieke cliënt, gaat het bij secundair gebruik om het hergebruik van gegevens voor andere doeleinden dan de doeleinden waarmee de gegevens aanvankelijk zijn verzameld, zoals zorgverlening. Bijvoorbeeld voor wetenschappelijk onderzoek, innovatie of beleidsvorming. In het EHDS-voorstel gaat het bij secundair gebruik om het toegankelijk maken van geanonimiseerde of gepseudonimiseerde gegevens, nooit direct tot een persoon herleidbare gegevens. Secundair gebruik van gezondheidsgegevens is belangrijk om goede, toegankelijke en betaalbare zorg te bevorderen en om preventie te ondersteunen. In mijn brief van 13 april 2023 over de *visie en strategie secundair gebruik* heb ik uw Kamer geïnformeerd over het belang van secundair gebruik van patiëntgegevens en welke stappen ik hierin wil gaan zetten. Het EHDS-voorstel sluit op grote lijnen goed aan bij die visie. Wel zijn in het voorstel bepaalde waarborgen nog vrij abstract, die moeten dus tijdens de onderhandelingen of bij de implementatie door de lidstaten worden uitgewerkt.

---

[11] Het CRA-voorstel betreft horizontale cyberbeveiligingsvereisten voor markttoelating van producten met digitale elementen waaronder ook EPD-systemen.

[12] Kamerstuk 22 112, nr. 3734.

Het EHDS-voorstel beoogt een geharmoniseerd raamwerk op te zetten in de gehele EU voor betere databeschikbaarheid voor secundair gebruik waarbij rekening wordt gehouden met waarborgen ter bescherming van de persoonlijke levenssfeer van betrokkenen. Dat moet er toe leiden dat verwerking van deze gegevens op een verantwoorde, veilige en transparante wijze gebeurt. In dit onderdeel over secundair gebruik licht ik de verschillende waarborgen toe.

Kaders voor toelaatbaar secundair gebruik

Het EHDS-voorstel beoogt een strikt kader te bieden waarbinnen secundair gebruik van gegevens kan plaatsvinden. Het voorstel kent geen verplichting om gegevens voor secundaire doeleinden exclusief via het EHDS-stelsel te verwerken. Als het niet via de EHDS wordt opgevraagd, is het reguliere kader van de (Uitvoeringswet)AVG en andere relevante wetgeving van toepassing, zoals momenteel het geval is. De EHDS-kaders geven weer wat de toelaatbare doeleinden zijn waarvoor gegevens kunnen worden gebruikt, en voor welke doeleinden gebruik expliciet verboden is.

Iedere aanvraag voor het beschikbaar stellen van data(sets) op basis van de EHDS wordt aan de hand van dit kader getoetst door de instantie voor toegang tot gezondheidsgegevens. Deze instantie wordt ook wel de *Health Data Access Body* genoemd (hierna: HDAB) en is een andere instantie dan de hiervoor genoemde digitale gezondheidsautoriteit. Indien voldaan wordt aan het kader dienen de gevraagde gegevens door de zogenaamde gegevenshouder beschikbaar te worden gesteld aan de HDAB. Het begrip «gegevenshouder» is breed gedefinieerd en omvat onder meer (publieke en private) zorgaanbieders en instellingen voor medisch-wetenschappelijk onderzoek. Voor het verstrekken van gegevens door deze gegevenshouders is geen voorafgaande toestemming van de burgers nodig. Zoals eerder aangegeven biedt deze wettelijke verplichting in het EHDS-voorstel al de benodigde juridische basis voor deze verstrekking van (persoons)gegevens.

Ieder gebruik dat buiten dit kader valt is niet toegestaan. Daarnaast blijven bestaande nationale ethische toetsen van toepassing. In het onderstaande kader worden de elementen uit het EHDS-toetsingskader nader toegelicht. Binnen dit kader moet de HDAB per aanvraag bepalen of een vergunning wordt verleend. De HDAB bepaalt in de vergunning ook welke specifieke maatregelen worden genomen om privacy en gegevensbescherming te waarborgen en houdt daarop toezicht.

Toetsingskader secundair gebruik (geparafraseerd)

Toelaatbare doeleinden (artikel 34)

Een aanvraag dient overeen te komen met één van de toelaatbare doeleinden op het gebied van de gezondheids- of zorgsector:
- beleids- en toezichtsdoeleinden (zowel nationaal als in EU verband) en andere activiteiten om redenen van algemeen belang op gebied van volksgezondheid en gezondheid op het werk;
- wetenschappelijk onderzoek;
- officiële statistieken;
- onderwijs;
- ontwikkeling van producten of diensten inclusief AI;
- leveren van gepersonaliseerde zorg door behandelaars (het mag niet gaan om gegevens van de patiënt zelf).

Verboden gebruiken (artikel 35)

De daartoe speciaal aangewezen HDAB toetst voor en na vergunningverlening of het gebruik van de gegevens binnen één van de verboden valt. De verboden zijn gericht op het beschermen van individuen, groepen en de maatschappij, en omvatten:
- besluiten nemen die nadelig zijn voor een burger op basis van hun gegevens;
- een verzekeringsovereenkomst ontzeggen of premies wijzigen.
- reclame- of marketingactiviteiten;
- toegang verlenen aan derden;
- producten of diensten ontwikkelen die schadelijk kunnen zijn voor personen of de samenleving.

Nationaal bepaalde ethische toets (artikel 45):

Een belangrijke additionele waarborg is de mogelijkheid voor lidstaten om een ethische toets te vereisen voor het verlenen van een vergunning die gepseudonimiseerde gegevens betreffen. Dit moet dan wel nationaal geregeld worden. Voor gepseudonimiseerde gegevens moet een aanvrager ook een grondslag aan kunnen tonen op basis van de AVG.

Voorbeelden secundair gebruik

Concrete voorbeelden van secundair gebruik kunnen zijn:
- wetenschappers die diepgravend onderzoek doen naar een nieuwe behandelmethode voor een zeldzame aandoening;
- een ontwikkelaar die een nieuw medisch hulpmiddel test op kwaliteit en effectiviteit;
- een toezichthouder die de gegevens nodig heeft voor het controleren van de veiligheid van geneesmiddelen op de markt;
- een beleidsmaker die statistieken laat produceren over doelmatigheid van beleidsinterventies.

Instantie voor secundair gebruik (HDAB)

Lidstaten worden verplicht om één of meerdere HDAB(s) voor toegang tot elektronische gezondheidsgegevens voor secundair gebruik op te zetten die verantwoordelijk is voor zowel operationele taken als toezichthoudende taken. Volgens het EHDS-voorstel hoeft de HDAB niet verplicht (onderdeel van) de eerder genoemde digitale gezondheidsautoriteit voor primair gebruik te worden. De operationele taken staan hoofdzakelijk ten dienste van het proces rondom de vergunningverlening, het beschikbaar stellen van bruikbare datasets aan vergunninghouders en de communicatie naar het bredere publiek.

De toezichthoudende taken richten zich specifiek tot de gegevenshouders en gegevensgebruikers. Aan de ene kant houdt de HDAB toezicht op naleving van de EHDS-verplichtingen omtrent het leveren van gegevens door gegevenshouders. Aan de andere kant houdt de HDAB toezicht op de gegevensgebruikers, bij de vergunningaanvraag en bij het verwerken van de gegevens. Gegevensgebruikers krijgen dus te maken met controle op de ontvankelijkheid en juistheid van hun aanvragen en daarna op gebruik conform de verleende vergunning. Verder ziet de HDAB erop toe dat de gebruiker geen poging doet tot het herleiden van een individuele burger. Op deze wijze wordt gewaarborgd dat gegevens altijd worden gebruikt voor doelen en afspraken overeenkomstig de verleende vergunning – in lijn met de voorwaarden van de EHDS en de AVG. Deze HDAB dient bij het

uitoefenen van haar toezichthoudende taken nauw samen te werken met de AP op vraagstukken die de privacy van burgers aangaan.

Vergunningstelsel voor secundair gebruik

De toegang tot gegevens van meerdere gegevenshouders voor secundair gebruik op basis van de EHDS kan alleen worden verleend indien een aanvrager een vergunning heeft verkregen van een HDAB (waarmee het een gegevensgebruiker wordt). De HDAB kan besluiten een vergunning niet te verlenen en voor bezwaar en beroep geldt het nationale recht. Zodra een vergunning is verstrekt krijgt een gegevensgebruiker via de HDAB toegang tot de gegevens in een beveiligde verwerkingsomgeving in geanonimiseerde of gepseudonimiseerde vorm (waarover hieronder meer). Zoals eerder aangegeven, moet dit volledige proces van vergunningsverstrekking altijd conform het gegevensbeschermingsrecht gebeuren. De verstrekte vergunningen gelden maximaal vijf jaar en mogen eenmalig worden verlengd met nogmaals maximaal vijf jaar. Na het verstrijken van de vergunning eindigt voor de gegevensgebruiker de toegang tot de gegevens en worden de tijdelijk opgeslagen anonieme of pseudonieme datasets verwijderd. De gegevensgebruikers zijn verplicht om de resultaten en/of output van het onderzoek of de innovatie openbaar te maken, uiteraard in een geanonimiseerde vorm.

De EHDS biedt met het vergunningstelsel een transparanter alternatief voor het huidige stelsel. Door de toegang centraal te coördineren en de toepassing van één toetsingskader wordt gewaarborgd dat toegang via de EHDS altijd op een geharmoniseerde en transparante wijze plaatsvindt. Dit in tegenstelling tot de huidige situatie waar het niet altijd duidelijk is onder welke omstandigheden gegevens worden verwerkt.

Vereisten aan beveiligde verwerking

Een gegevensgebruiker krijgt alleen toegang tot gegevens in een verwerkingsomgeving die voldoet aan de EHDS-beveiligingsvereisten. In deze «digitale kluis» heeft de HDAB controle over de verwerking van de gegevens. Hierin worden datasets, waar nodig, door de HDAB gekoppeld en wordt herleidbaarheid geminimaliseerd, zodat de gebruiker alleen toegang krijgt tot versleutelde en/of geaggregeerde gegevens. Pas nadat dit gewaarborgd is, krijgt de gegevensgebruiker toegang. Elke individuele onderzoeker en verwerking wordt gelogd. Dergelijke omgevingen zijn niet nieuw in Nederland: deze werkwijze wordt reeds gebruikt bijvoorbeeld door het CBS voor toegang door onderzoekers.

De beveiligde verwerkingsomgeving maakt het mogelijk voor de HDAB om toezicht te houden en om in te grijpen als gegevens onverhoopt oneigenlijk worden gebruikt. De HDAB moet bij onrechtmatig gebruik ingrijpen en sanctioneren, zoals het intrekken van de vergunning. De HDAB kan de gegevensgebruiker vervolgens maximaal 5 jaar uitsluiten van elke toegang tot gezondheidsgegevens. Verder kunnen lidstaten extra sancties introduceren voor een poging tot het herleiden van personen.

De HDAB moet dus over (één of meer) beveiligde verwerkingsomgeving(en) beschikken en moet deze regelmatig auditen. De beveiligde verwerkingsomgeving moet voldoen aan technische en organisatorische vereisten:
– voldoen aan de hoogste (geharmoniseerde) beveiligingsstandaarden;
– gegevensgebruikers krijgen alleen toegang tot de gezondheidsgegevens waarop hun vergunning betrekking heeft;
– beperken van het risico op onrechtmatig lezen en verwerken, zoals kopiëren, wijzigen of weghalen van gegevens. Dat moet worden

gedaan met behulp van geavanceerde technologische middelen (zoals *privacy enhancing technologies)*;
– bijhouden van identificeerbare toegangslogs.

Algemene transparantie en rechten van personen

Het EHDS-voorstel voorziet in vereisten voor transparantie. Op de website van de HDAB moet informatie te vinden zijn over de uitgegeven vergunningen, de waarborgen, en resultaten uit secundair gebruik. Burgers moeten op de website ook de regelingen kunnen vinden om hun AVG-rechten uit te oefenen (bijv. recht op inzage, rectificatie of bezwaar), rechten die blijven gelden bij secundair gebruik.

Het huidige EHDS-voorstel kent geen verplichting om burgers op individueel niveau te informeren over verwerking van gegevens op basis van een vergunning, maar de ruimte is er voor lidstaten om dit te regelen. In de onderhandelingen is een meerderheid van de lidstaten van mening dat het uitblijven van de plicht om burgers te informeren over verwerking van hun persoonsgegevens door de HDAB niet verenigbaar is met het principe van transparantie en het recht om bezwaar te kunnen maken. Daarnaast wordt in het voorstel geen duidelijke mogelijkheid geboden voor burgers om bezwaar te maken tegen secundair gebruik. In de Raad wordt daarom geïnventariseerd welke mogelijkheden er zijn om het bezwaarrecht (AVG) duidelijker vorm te geven in de EHDS.

Inbedding van dataminimalisatie

Het EHDS-voorstel past in de vergunningensystematiek dataminimalisatie toe. Dit AVG-beginsel gaat ervan uit dat bij verwerking van persoonsgegevens een minimale hoeveelheid gegevens wordt gebruikt om het beoogde doel te bereiken. Dataminimalisatie wordt op ten minste drie manieren toegepast in het EHDS-voorstel.

Ten eerste verzoekt de HDAB bij de houder alleen toegang tot de datasets die nodig zijn voor het doel dat in de verstrekte vergunning staat vermeld. Op verzoek van de HDAB dient een gegevenshouder het desbetreffende deel van de dataset toegankelijk te maken voor de HDAB. Waar de HDAB het nodig acht dat de gegevens door de gebruiker verwerkt worden, gebeurt dit altijd in de beveiligde verwerkingsomgeving.

Ten tweede, om het risico tot herleiding van personen te minimaliseren, stelt de EHDS dat het bindende «anoniem, tenzij» principe geldt. De gegevens die verwerkt worden door de gegevensgebruiker zijn daarmee standaard anoniem en alleen pseudoniem indien de HDAB constateert dat dat noodzakelijk is om het doel van de vergunning te bereiken. Daarbij gelden wel aanvullende veiligheidsmaatregelen waardoor gegevensgebruikers nooit over de koppelingssleutel kunnen beschikken waarmee de gegevens herleidbaar zijn tot een individu.

Ten derde blijft in geval van grensoverschrijdende aanvragen de Nederlandse HDAB het enige bevoegde orgaan dat buitenlandse gegevensgebruikers toegang kan verlenen tot gepseudonimiseerde of geanonimiseerde gegevens uit Nederland. Het EHDS-voorstel vereist wel dat toegang verleend moet worden als de aanvrager voldoet aan het toetsingskader. In dergelijke gevallen kan op afstand toegang gegeven worden in een Nederlandse beveiligde verwerkingsomgeving onder toezicht van de Nederlandse HDAB.

Slot

Het EHDS-voorstel stelt regels die gezondheidsgegevens in de EU op een veilige en verantwoorde manier breder beschikbaar maken voor primair en secundair gebruik. Het EHDS-voorstel voorziet in een juridische basis voor het verwerken van de gegevens en creëert waarborgen. Net als in de nationale visie en strategie is aangegeven is voor toegang tot gegevens het vertrouwen van burgers in een integere omgang met de gezondheidsgegevens randvoorwaardelijk. In deze brief heb ik uw Kamer zo feitelijk mogelijk geïnformeerd over de waarborgen uit het EHDS-voorstel waarover nog wordt onderhandeld. Het EHDS-voorstel zie ik als een bouwsteen om samen te werken aan een toekomstbestendig gezondheidsinformatiestelsel. In de onderhandelingen blijf ik mij hard maken voor de eerder gecommuniceerde onderhandelingsinzet van Nederland. Zodra er meer bekend is over de uitkomsten van de onderhandelingen, informeer ik uw Kamer hierover.

De Minister van Volksgezondheid, Welzijn en Sport,
E.J. Kuipers