ZAURUS

Whitepaper

Veilige digitale gegevensuitwisseling in de zorg

Inleiding

Nu het post-corona tijdperk in zicht lijkt te komen, is het hoogstwaarschijnlijk dat de digitale gegevensuitwisseling in de zorg niet meer weg te denken is. Sterker nog, de komende jaren zal de digitale gegevensuitwisseling in de zorg zich nog verder ontwikkelen en een onlosmakelijk onderdeel uitmaken van zorgprocessen.

Gedurende de corona-pandemie hebben zorgaanbieders reeds kennis gemaakt met communicatieaanbieders op het gebied van onder andere veilig beeldbellen, chatten en audiobellen. In de haast is destijds een keuze gemaakt voor een passende leverancier. Nu de rust is wedergekeerd is het tijd om keuzes te herijken en andere opties te onderzoeken.

In deze publicatie staat Zaurus stil bij soorten digitale gegevensuitwisseling, de relevante en geldende wetgeving, waarbij veel nadruk zal worden gelegd op de privacywetgeving (de Algemene verordening gegevensbescherming). Wat zegt de wet, hoe passen leveranciers dit toe, waar moet je op letten bij het kiezen van een nieuwe leverancier? We eindigen de publicatie met een conclusie en toepasselijke aanbevelingen.

Soorten digitale gegevensuitwisseling in de zorg

Digitale gegevensuitwisseling in de zorg is op te splitsen in twee varianten:

- Gegevensuitwisseling met de patiënt;
- Gegevensuitwisseling tussen zorgaanbieders. Hierbij wordt er onderscheid gemaakt tussen pull- en push-verkeer. Bij push-verkeer ligt het initiatief voor het verzenden van informatie bij de verzender die de patiëntgegevens naar één ontvanger verstuurd. Bij pull-verkeer stelt een arts een patiëntendossier of gegevens daaruit beschikbaar voor raadpleging door andere zorgverleners. Hierbij is het vooraf niet duidelijk wie de gegevens zullen raadplegen.

Juridisch kader veiligheid gegevensuitwisseling in de zorg

Veiligheid van informatie is uiterst belangrijk, zeker in de zorg. In de zorg worden medische gegevens gedeeld, welke vallen onder de categorie “bijzondere persoonsgegevens”. Deze categorie van informatie moet streng worden beveiligd. Met betrekking tot de zorg kunnen we een aantal relevante wetten toepassen, namelijk:

- Wet op de geneeskundige behandelingsovereenkomst (WGBO).
- Algemene verordening gegevensbescherming (AVG);
- Wet aanvullende bepalingen gegevensverwerking in de zorg (Wabpz)
- Wetsvoorstel: Wet elektronische gegevensuitwisseling in de zorg (Wegiz)

WGBO (BW) Artikel 7:446

“De overeenkomst inzake geneeskundige behandeling […] is de overeenkomst waarbij een natuurlijke persoon of een rechtspersoon, de hulpverlener, zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde. […]” (Overheid, 2021)

Er mogen alleen gegevens worden gedeeld tussen een zorgverlener en zorgvrager als er een (behandelings)overeenkomst tussen beiden is gesloten of indien een zorgvrager toestemming heeft gegeven om gegevens te delen met derden.

WGBO (BW) Artikel 7:456

"De hulpverlener verstrekt aan de patiënt desgevraagd inzage in en afschrift van de gegevens uit het dossier. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander." (Overheid, 2021).

Deze bepaling gaat over het recht op inzage van het medisch dossier. Een zorgvrager heeft recht op inzage van het medisch dossier. Hierop geldt één uitzondering: als de privacy van een ander (dan de zorgvrager) door inzage wordt geschaad.

WGBO (BW) Artikel 7:457

"1 Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de gegevens uit het dossier worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.

2 Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden." (Overheid, 2021).

Zorgverleners hebben een beroepsgeheim. Een zorgverlener moet zwijgen over alles wat hij/zij tijdens het werk te weten komt over een zorgvrager. Zo wordt het vertrouwen niet geschaad en blijft de vertrouwelijkheid van informatie geborgd. Een uitzondering op deze geheimhoudingsplicht is voor zorgverleners die rechtstreeks betrokken zijn, waarnemers (7:457 lid 2 BW) en in het kader van een verwijzing.

AVG Artikel 9 lid 1

"[…] verwerking van gegevens over gezondheid […] zijn verboden." (Europese Unie, 2021)

De verwerking van bijzondere persoonsgegevens (waaronder gegevens over gezondheid – c.q. medische gegevens) is verboden, behoudens de uitzonderingen gegeven in artikel 9 lid 2 AVG.

AVG Artikel 9 lid 2

In artikel 9 lid 2 van de AVG worden uitzonderingen gegeven waarop bijzondere persoonsgegevens (waaronder medische gegevens) wel mogen worden verwerkt, waaronder toestemming en een eis met betrekking tot de verwerking en de beveiliging van informatie. (Europese Unie, 2021)

AVG Artikel 32 lid 1

" […] treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen […]" (Europese Unie, 2021)

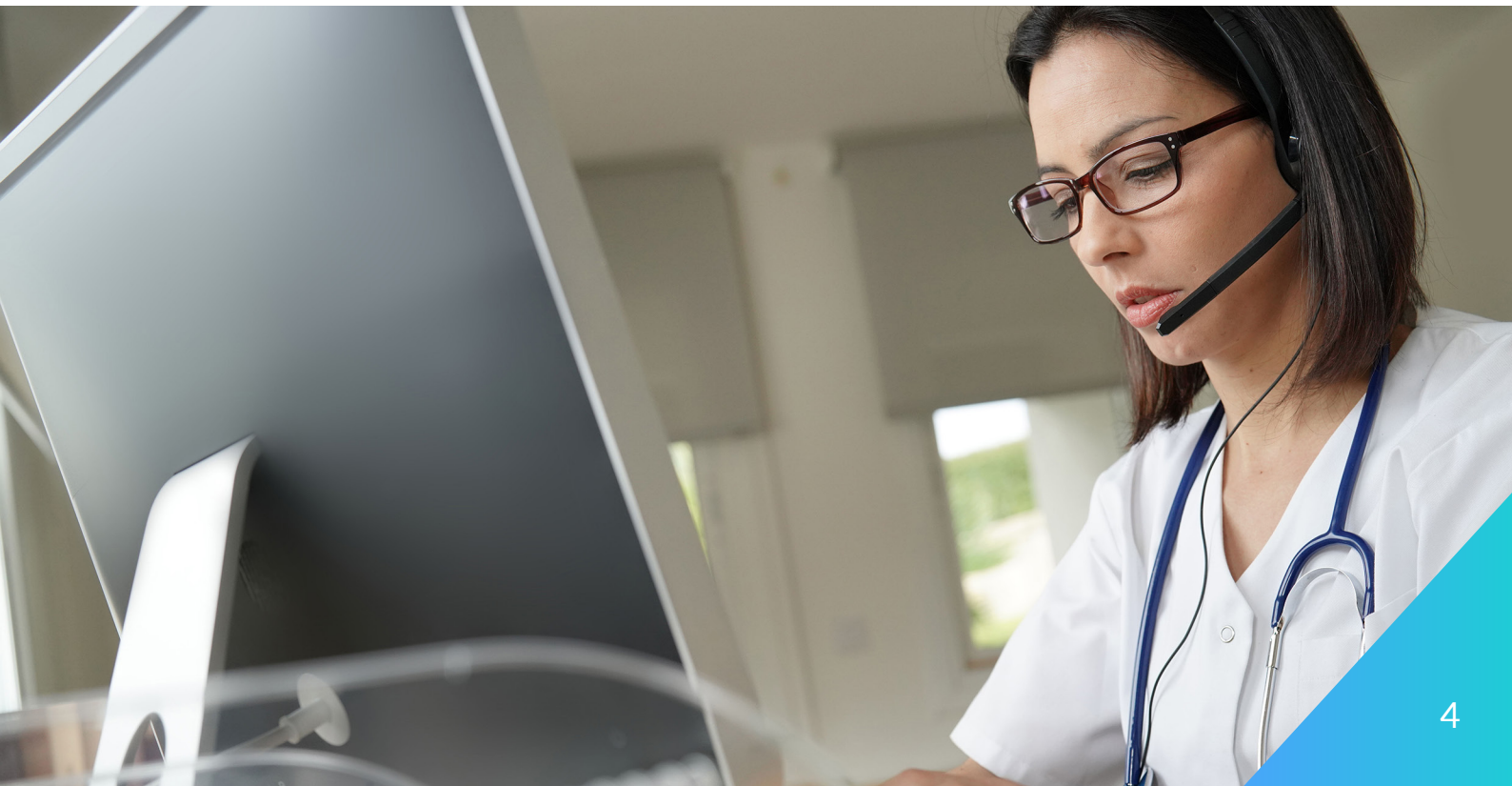
Afhankelijk van onder andere de aard en de omvang van de informatie die digitaal wordt gedeeld, dient deze informatie adequaat te worden beveiligd. Later in deze publicatie geven wij enkele richtlijnen waar leveranciers van communicatie-oplossingen op kunnen worden getoetst.

Wabpz Artikel 15a lid 1 en lid 3

"De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselingssysteem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven."

"De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselingssysteem, voor zover bij het raadplegen van die gegevens door een andere zorgaanbieder, de persoonlijke levenssfeer van een ander dan de cliënt niet wordt geschaad."

Er mogen pas gegevens worden gedeeld, zodra de zorgvrager toestemming heeft gegeven. De uitwisseling mag de privacy van een persoonlijke levenssfeer niet schaden.



Bepalen van de risico's

In de AVG is vastgelegd dat onder andere een risicoanalyse moet worden uitgevoerd indien het gaat om een gegevensverwerking welke waarschijnlijk een hoog privacyrisico oplevert voor de personen van wie de organisatie gegevens verwerkt (i.e. de betrokkenen).

Concreet: een zorgverlener die op zoek gaat naar een (nieuwe) leverancier voor digitale gegevensuitwisseling (waarbij medische gegevens worden verwerkt) zal onder andere een risicoanalyse moeten maken om vooraf de privacyrisico's van de gegevensverwerking in kaart te brengen en om vervolgens (beveiligings)maatregelen te treffen om deze risico's te verkleinen.

Een dergelijke risicoanalyse wordt een Data Protection Impact Assessment (DPIA) genoemd. In een DPIA beoordeelt de zorgaanbieder de leverancier onder andere op beveiliging en privacy.

"Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking oplevert voor de betrokkenen. En in de maatregelen die u moet nemen om de risico's af te dekken. Het is aan u om die maatregelen ook daadwerkelijk te treffen. Of eventueel een voorafgaande raadpleging aan te vragen.

Als er een functionaris gegevensbescherming (FG) is, moet u bij het uitvoeren van een DPIA het advies van de FG inwinnen. Dit geeft extra zekerheid dat de DPIA voldoende zicht geeft op de risico's en er voldoende maatregelen worden getroffen om deze af te dekken."

De Autoriteit Persoonsgegevens
Nederlandse toezichthouder op de privacywetgeving
(AP, Data protection impact assessment (DPIA), 2021).

Selectiecriteria leveranciers digitale gegevensuitwisseling in de zorg

Bij het uitvoeren van een risicoanalyse moet onder andere worden beoordeeld of de technische en organisatorische maatregelen, die de leverancier heeft getroffen, voldoende worden geacht om de informatie te beschermen. Echter, waar moet je als zorgaanbieder dan op letten?

NEN 7510 en ISO 27001

Er zijn veel misvattingen over de verplichting van de NEN 7510. Om te weten wat de NEN 7510 precies inhoudt, is het verstandig om te beginnen met de ISO 27001.

De ISO 27001 is een internationale norm waarin regels worden gesteld over hoe je informatie moet beveiligen. Deze regels bestaan uit het oprichten van een (management)systeem wat informatiebeveiliging moet borgen binnen alle (relevante) processen in de bedrijfsvoering. Daarnaast worden in de norm heel erg veel maatregelen gesteld die een leverancier wel/niet kan toepassen. Een leverancier verklaart in zijn (openbaar of opvraagbaar) verklaring van toepasselijkheid in hoeverre de norm is toegepast. Met andere woorden: welke maatregelen zijn wel of niet geïmplementeerd.

Tip!

Vraag dus altijd de verklaring van toepasselijkheid op bij een leverancier om goed inzicht te krijgen welke maatregelen wel/niet zijn geïmplementeerd.

De ISO 27001 is een standaard die in vrijwel elke branche kan worden gebruikt. Echter, in Nederland bestond een behoefte om deze norm uit te breiden met extra maatregelen, specifiek voor de zorg. Om deze reden is de NEN 7510 tot stand gekomen. Deze norm is identiek aan de ISO 27001, met als uitzondering dat daar extra regels in staan om de beveiliging van informatie in de zorg nog meer te kunnen garanderen.

Zoals eerder toegelicht in het juridisch kader, verplicht de AVG dat er een risicoanalyse plaatsvindt op onder andere de technische en organisatorische maatregelen die door een leverancier zijn getroffen. Een manier waarop leveranciers dit kunnen aantonen, is door middel van een certificaat, bijvoorbeeld het NEN 7510 certificaat. Een onafhankelijke, certificerende instelling (i.e. auditbedrijf) toetst of het bedrijf de norm goed heeft toegepast. Indien dit het geval is, zal de leverancier hiervan een certificaat bemachtigen. Een certificaat zegt dus in enige mate iets over hoe de beveiliging binnen een organisatie is geborgd.

De AP stelt: *"Certificering volgens de NEN 7510 is op grond van de AVG niet verplicht. Ongeacht de rechtsvorm en de omvang van uw organisatie. De NEN 7510 blijft onder de AVG wél een belangrijke norm voor informatiebeveiliging in de zorg. Op dit moment geldt bijvoorbeeld dat u aan de NEN 7510 moet voldoen als u in de zorg het burgerservicenummer (BSN) verwerkt."* (AP, Zorgverleners en de AVG, 2021). Deze verplichting vloeit voort uit artikel 2 - Regeling gebruik burgerservicenummer in de zorg.

Let op! Leveranciers die spreken over 'wij houden ons aan NEN 7510' of 'wij werken volgens ISO 27001' beschikken niet altijd over een certificaat. Raadpleeg het NEN-register (NEN, 2021) of vraag de leverancier naar het certificaat en de verklaring van toepasselijkheid.

Gegevensverwerking – omgang met persoonlijk identificeerbare informatie

Een andere manier om te kijken naar de veiligheid van digitale gegevensuitwisseling, is om ook de gegevensverwerking van de leverancier onder de loep te nemen. Welke gegevens verwerkt de leverancier? Waar vindt de verwerking plaats? Met wie wordt informatie gedeeld? Etc.

Tip!

Veel van dit soort informatie is terug te vinden op de websites van de leveranciers. Controleer webpagina's over privacy, compliance of informatiebeveiliging. Lees de privacy- en cookieverklaring goed door.

Daarnaast is het natuurlijk uitermate belangrijk om een verwerkersovereenkomst te sluiten. Als zorgverlener bent u (in veel gevallen) verwerkingsverantwoordelijke en daarmee verantwoordelijk voor de informatie (waaronder persoonsgegevens) en met wie (en onder welke voorwaarden) u deze informatie deelt. Immers, u bepaalt het doel van en de middelen die u gebruikt voor de verwerking van persoonsgegevens.

Let op! Een verwerkersovereenkomst hoeft niet per definitie een separate overeenkomst te zijn. Leveranciers kunnen er ook voor kiezen om informatie te geven over verwerkingen in de algemene overeenkomst, in een bijlage of via bepalingen in de algemene voorwaarden.

Tip!

Binnen de zorg bestaat een standaard template voor een verwerkersovereenkomst die breed in de branche wordt gebruikt. (Brancheorganisaties Zorg, 2021)

Een verwerkersovereenkomst moet volgens de AVG bestaan uit verplichte elementen. Raadpleeg artikel 30 van de AVG om de verwerkersovereenkomst te toetsen of laat de verwerkersovereenkomst toetsen door een jurist met kennis van privacy. (Europese Unie, 2021)

Ook is er een ISO-norm voor de veilige omgang van persoonsgegevens beschikbaar waar onder andere leveranciers zich op kunnen laten toetsen. De NEN-ISO/IEC 27701 is een aanvulling op de eerdergenoemde ISO 27001. De ISO 27001 richt zich op beveiligingsmaatregelen, terwijl de ISO 27701 zich richt op additionele maatregelen ten behoeve van de privacy van betrokkenen. De ISO 27701 kan informatie bieden over hoe privacy binnen de organisatie van een leverancier is ingebed. Vraag wederom weer om de verklaring van toepasselijkheid om te weten te komen welke maatregelen zijn ingebed in de organisatie en getoetst door de certificerende instelling.

Privacy by default en Privacy by design

Vraag in een gesprek met de leverancier naar hoe “privacy by design” en “privacy by default” zijn toegepast.

- Privacy by default houdt in dat het communicatiemiddel de meest veilige optie als standaard aanbiedt. Dit kan eventueel door de gebruiker/beheerder worden aangepast. Met andere woorden: de standaardinstellingen van de applicatie worden bij aanvang zo privacyvriendelijk mogelijk ingesteld, maar bieden wel mogelijkheden om dit te verruimen. Bijvoorbeeld: tweestapsverificatie staat standaard aan voor alle gebruikers, gebruikers worden verplicht om een sterk wachtwoord te kiezen en dit periodiek te wijzigen etc.

- Privacy by design houdt in dat tijdens het ontwikkelproces de leverancier zich al bezighoudt met hoe de privacy (en informatiebeveiliging) wordt geborgd. Indien bijvoorbeeld iets in de applicatie wordt gebouwd welke een hoog risico oplevert voor betrokkenen, wordt de functionaris gegevensbescherming, privacy officer of informatiebeveiligingsspecialist (afhankelijk van beschikbare disciplines binnen een organisatie) erbij gehaald om advies te geven. Aan de hand van dit advies wordt er richting gegeven aan de ontwikkeling.

Andere aandachtspunten

Type oplossing ten behoeve van digitale gegevensuitwisseling

Er zijn veel manieren om gegevens digitaal uit te wisselen. In de markt zijn dan ook veel type oplossingen te vinden voor verschillende, en soms meerdere, manieren van digitale gegevensuitwisseling. In deze whitepaper wordt specifiek stilgestaan bij digitale gegevensuitwisseling middels beeldbellen. In onderstaande secties wordt conform de geïdentificeerde categorieën van Smarthealth (Smarthealth, 2021) onderscheid gemaakt tussen consumenten beeldbeloplossingen, zakelijke beeldbeloplossingen en beeldbeloplossingen specifiek voor de zorg. Per oplossing worden de voor- en nadelen onder de loep genomen.

1. Consumenten beeldbeloplossingen;

Voorbeelden van consumentenoplossingen zijn Skype, Facetime en WhatsApp. Deze diensten zijn vaak gratis. **Let op!** Vaak betaal je indirect doordat een gebruiker akkoord gaat dat bepaalde gegevens mogen worden verwerkt.

Consumentenoplossingen voldoen **niet geheel** aan de beveiligingseisen die wet- en regelgeving daaraan stellen (AVG, NEN en ISO-normen voor informatiebeveiliging in de zorg). Het gebruik van WhatsApp is in 2016 al door de AP afgeraden (ICTRecht, 2021). De AP adviseert zorgaanbieders ook te kijken naar de tips voor beeldbellen van de NEN, KNMG en LVVP. (AP, Keuzehulp privacy bij videobel-apps, 2021). Echter, uit de publicatie van het KNMG (KNMG, 2020) blijkt dat het gebruik van WhatsApp alleen door artsen is toegestaan mits de gegevens niet te herleiden zijn naar een zorgvrager. Dit is heel lastig, omdat vaak bij het uitwisselen van data gebruik wordt gemaakt van metadata (bijv. kenmerken aan een foto), zodat de zorgvrager alsnog kan worden herleid. Het gebruik van consumentenproducten voor medische inhoud lijkt niet heel verstandig.

"Veel gebruikte consumententoepassingen als Skype, Facebook Messenger en WhatsApp voldoen mogelijk niet aan alle wettelijke beveiligingseisen voor het uitwisselen van gezondheidsinformatie. Als het niet anders kan, kan de arts deze toepassingen gebruiken, maar het advies is om veiligere toepassingen te gebruiken als die voorhanden zijn."

Artsenfederatie KNMG

Koninklijke Nederlandse Maatschappij tot bevordering der Geneeskunst

2. Zakelijke beeldbeloplossingen;

Zakelijke oplossingen zijn bijvoorbeeld Zoom, Microsoft Teams, Google, WebEx, Skype, Wereby en Google Hangouts. Deze communicatieoplossingen zijn specifiek ontwikkeld voor de zakelijke markt. Omdat deze applicaties niet specifiek voor de zorg ontwikkeld zijn, is het niet duidelijk in hoeverre ze aan wettelijke eisen van de AVG, NEN en ISO-normen voor informatiebeveiliging in de zorg voldoen. Zo bewees ook een recent artikel (7 juni 2021) van het Financieel Dagblad:

"Toezichthouder maant scholen, universiteiten en Justitie om met Google te stoppen (Financieel Dagblad, 2021)." (Financieel Dagblad, 2021). Volgens de AP voldoet de software van Google niet aan de AVG.

3. Zorgspecifieke beeldbeloplossingen.

Denk hierbij bijvoorbeeld aan de oplossingen van Zaurus. Zaurus biedt een zorgspecifieke oplossing en is ontwikkeld om aan de wettelijke eisen en normen te voldoen. Zorgaanbieders betalen voor de applicatie, maar weten dat er goed wordt omgegaan met privacy en informatiebeveiliging. Het gebruik van de applicatie is voor de daadwerkelijke zorgvragers gratis.

De AP adviseert zorgaanbieders te kijken naar de tips voor beeldbellen van de NEN, KNMG en LVVP. (AP, Keuzehulp privacy bij videobel-apps, 2021). Zaurus is opgenomen in deze keuzehulpen. Uiteraard staan wij je graag te woord om je meer informatie te geven over de mogelijkheden en beveiliging van oplossingen.

Herkomst van de leverancier

Iets wat momenteel heel erg speelt, is de locatie van de verwerking. Dit klinkt misschien onlogisch, maar is eigenlijk heel erg verstandig en belangrijk om te weten!

Volgens artikel 45 van de AVG kunnen persoonsgegevens worden doorgegeven aan landen buiten de Europese Economische Ruimte (EER) wanneer de Europese Commissie heeft besloten dat dat derde land een passend niveau van gegevensbescherming biedt. De Europese Economische Ruimte (EER) omvat alle EU-landen plus Liechtenstein, Noorwegen en IJsland.

Met andere woorden: data mogen de EER alleen maar verlaten naar een ander land buiten de EER, indien dit land dezelfde garanties kan bieden, zoals deze gelden binnen de EER.

Verenigde Staten

Veel populaire leveranciers van oplossingen ten behoeve van digitale gegevensuitwisseling (Zoom, WhatsApp, Microsoft Teams, Slack etc.) vinden hun oorsprong in de Verenigde Staten van Amerika (VS). Voorheen waren afspraken omtrent de uitwisseling van gegevens tussen de VS en de EER vastgelegd in het "Privacy Shield". Bedrijven in de VS konden zich conformeren aan de regels van het Privacy Shield en op basis hiervan informatie uitwisselen met de EER. Echter, op 16 juli 2020 heeft het Hof van Justitie EU het Privacy Shield ongeldig verklaard in de zaak "Schrems II". Organisaties in de Europese Unie (EU) mogen geen persoonsgegevens meer aan de Verenigde Staten doorgeven op grond van het Privacy Shield.

Veel Amerikaanse leveranciers (van digitale gegevensuitwisseling) hebben of maken gebruik van een Amerikaans datacenter (i.e. cloud provider) binnen Europa. Daarmee beweren zij dat data binnen de EER blijven en zij hiermee conformeren aan geldende wet- en regelgeving (waaronder de AVG).

Waar zit dan het probleem? Zoals AKD Benelux laywers stelt: *"In maart 2018 is in de Verenigde Staten ("VS") de US CLOUD Act aangenomen. Deze wet staat voor 'Clarifying Lawful Overseas Use of Data' en geeft Amerikaanse autoriteiten de bevoegdheid om gegevens op te vragen bij bedrijven die in de VS elektronische communicatiediensten of remote computing-diensten aanbieden. Dergelijke gegevens hoeven hiervoor niet in de VS te zijn opgeslagen. Deze wetgeving kan dus vergaande gevolgen hebben voor zowel Nederlandse burgers omdat hun persoonsgegevens kunnen worden gedeeld met de VS, als voor Nederlandse bedrijven omdat zij mogelijk in een juridische spagaat terecht kunnen komen."* (AKD benelux laywers , 2020)

Een Amerikaanse leverancier kan dus, op grond van een gerechtelijk bevel, worden verplicht om gegevens (waaronder persoonsgegevens) door te geven. Hiermee staat de US CLOUD Act recht tegenover de AVG. De leveranciers zitten in een spagaat. Gaan zij zich conformeren aan de AVG of aan de US CLOUD Act?

ICTRecht beargumenteert: *"Op grond van artikel 48 van de AVG is het cloud providers met een vestiging in de EU uitdrukkelijk verboden om gehoor te geven aan verzoeken of bevelen van autoriteiten van landen buiten de EU [...]. Wanneer een cloud provider gehoor zou geven aan een vordering van een Amerikaanse autoriteit die op basis van de CLOUD Act rechtstreeks aan de Amerikaanse vestiging van de cloud provider is gericht, in plaats van aan de autoriteiten van het vestigingsland in de EU [...] tot het verstrekken van klantdata waaronder zich medische data van Nederlandse patiënten bevinden, dan zou de cloud provider in overtreding zijn van de AVG. Op deze overtreding is het hoge boetemaximum van de AVG (20.000.000 euro of 4% van de wereldwijde jaaromzet) van toepassing."* (ICTRecht, 2019)

Hoewel voorgaand citaat zich richt op cloud providers, geldt hetzelfde principe voor aanbieders van digitale communicatieoplossingen.

In verwerkersovereenkomsten hebben veel Amerikaanse leveranciers extra bepalingen opgenomen om de veiligheid van informatie te kunnen waarborgen op dit vlak. Echter, of deze bepalingen voldoen is nog maar de vraag. Op 4 juni 2021 zijn door de Europese Commissie nieuwe contractuele bepalingen gepubliceerd waaraan leveranciers buiten de EER kunnen conformeren. In hoeverre Amerikaanse leveranciers hieraan voldoen is nog niet duidelijk. Dit zal de komende maanden de nodige aandacht krijgen.

Daarnaast is het goed om te weten dat op 27 mei 2021 de European Data Protection Supervisor (EDPS) is begonnen met o.a. een onderzoek met betrekking tot het gebruik van cloud services die worden aangeboden door diverse niet-Europese cloud leveranciers. Het doel van het onderzoek is om de naleving van het "Schrems II"-arrest te beoordelen bij het gebruik van cloud services die worden geleverd door diverse niet-Europese cloud providers onder de zogenaamde "Cloud II-contracten" wanneer gegevens worden overgedragen naar niet-EU-landen, met name naar de VS.

Microsoft berichtte mei 2021 het volgende: *"Wij bevestigen vandaag opnieuw een plechtige belofte tegenover de Europese Unie. […] Anders gezegd: wij zullen uw gegevens niet meer buiten de EU versluizen. […] We gaan onmiddellijk aan de slag voor deze extra stap en we zullen tegen het einde van volgend jaar klaar zijn met de implementering van alle engineering die vereist is voor de voltooiing hiervan. Dit plan krijgt de naam 'EU Data Boundary for the Microsoft Cloud".* (Microsoft, 2021)

Data-uitwisseling met Amerikaanse partijen is op dit moment complex in juridische zin. Er kunnen geen harde garanties worden afgegeven over de vertrouwelijkheid van de data. Een oplossing laat op zich wachten. Momenteel ontstaan in Europa initiatieven om Europese datacenters op te richten, waardoor datacenters in Europese handen komen en data conform de AVG kunnen worden verwerkt. Een voorbeeld van een dergelijk initiatief is het GAIA-X project. *"GAIA-X is een project geïnitieerd door Europa voor Europa en daarbuiten. Het doel is om gemeenschappelijke eisen te ontwikkelen voor een Europese data-infrastructuur. Daarom staan openheid, transparantie en verbinding met andere Europese landen centraal bij GAIA-X."* (GAIA-X, 2021).

Zolang Europese initiatieven nog niet tot iets concreets leiden, wordt afnemers geadviseerd om maatregelen te treffen die bij kunnen dragen aan een passend beveiligingsniveau. Indien er voor een Europese aanbieder wordt gekozen, kan in ieder geval de AVG van toepassing worden verklaard, worden gehandhaafd en nageleefd.

Overige punten

Naast bovengenoemde punten geven wij nog enkele overige richtlijnen, tips en trucs mee.

- Controleer hoe het beheer van versleuteling is geregeld. Ligt het beheer bij de zorgverlener of bij de leverancier?
- Controleer welke gegevens door de leverancier worden verzameld. Een overzicht van de Autoriteit Persoonsgegevens laat zien dat bij Facetime onder andere locatiegegevens en gegevens over gesprekken worden verzameld (AP, Keuzehulp privacy bij videobel-apps, 2021). De medisch gerelateerde contacten met cliënten en de gegevens die daarin worden verwerkt moeten echter strikt privé blijven. Het verzamelen en verwerken van deze gegevens voor andere redenen dan het leveren van zorg kan in strijd zijn met de AVG.
- Controleer of de leverancier middels een applicatie ook toegang heeft tot overige gegevens op het draagbare apparaat (bijv. telefoon, tablet, laptop). Wat staat er in de gebruiksvoorwaarden hierover afgesproken? Mag WhatsApp contactgegevens doorgeven aan bijv. Facebook?
- Hoe slaat de leverancier de gegevens op het mobiele apparaat op? Indien je een applicatie gebruikt op privéapparaten, worden dan bijv. privé en zakelijke gegevens met elkaar gecombineerd? Bijvoorbeeld: staat informatie (bijv. foto's) van zorgvragers tussen privé-informatie (galerij met foto's)? In dat geval, waar slaat dit individu zijn gegevens op? Bijv. OneDrive, Dropbox etc. Let op! Er is een vergrootte kans op datalekken en overschrijding van de AVG als scheiding prive en zakelijk verdwijnt.
- Controleer of de leverancier daadwerkelijk NEN 7510 gecertificeerd is via de website van het NEN. (NEN, 2021)

Gevolgen

Het niet naleven van de AVG kan leiden tot reputatieschade, een waarschuwing van de AP of een boete.

Wat vinden de politiek, de toezichthouder en brancheorganisaties?

Politiek

In 2019 heeft voormalig minister voor Medische Zorg en Sport, Dhr. B. Bruins, een onderzoek laten verrichten naar opslag van medische data in de cloud. In zijn brief naar de voorzitter van de Tweede Kamer schrijft hij het volgende:

"Uit het onderzoek dat ik heb laten verrichten, is naar voren gekomen dat het wenselijk is om gebruik te maken van een cloud provider met een vestiging, vertegenwoordiging of opslagcapaciteit binnen de Europese Unie. Op deze cloud providers is immers de AVG van toepassing. Hiermee worden de data beschermd tegen onrechtmatig gebruik door de cloud provider en kan naleving van de AVG effectief worden afgedwongen. […] De onderzoekers adviseren daarnaast om het versleutelen van de informatie vóór deze in de cloud geplaatst wordt, waardoor er sprake is van een dubbele versleuteling." (Rijksoverheid, 2019).

De Europese Commissie werkt toe naar een opvolger van het Privacy Shield, maar dit proces is langdurig en het zal dus nog even duren voordat het echt duidelijk is onder welke voorwaarden data mogen worden gedeeld met de Verenigde Staten. (CNBC, 2021)

Toezichthouder

De AP refereert voor tips voor veilige digitale gegevensuitwisseling naar de websites van onder andere het LVVP en KNMG.

- Tips van het LVVP
- Tips van de KNMG

Brancheorganisatie KNMG

"Er zijn speciaal voor de zorg ontwikkelde toepassingen voor beeldbellen beschikbaar. Naar verwachting is bij de ontwikkeling hiervan gelet op de wettelijke eisen en normen voor het uitwisselen van gevoelige zorginformatie. Die eisen en normen vloeien met name voort uit de AVG en uit de NEN- en ISO-normen voor informatiebeveiliging in de zorg." (KNMG, 2020)

LHV, InEén en NHG hebben gezamenlijk een overzicht gemaakt van bestaande zorgtoepassingen en andere beeldbelapplicaties, waarin deze op verschillende criteria zijn vergeleken.

Concluderend

Het verdient aanbeveling om bij het kiezen voor een leverancier met betrekking tot digitale gegevensuitwisseling (beeldbellen, chatten, audiogesprekken etc.) te letten op welk type applicatie zij bieden en hoe dit beveiligd is. Idealiter wordt een aanbieder gekozen welke specifiek een applicatie heeft gemaakt voor de zorg, welke minstens NEN 7510 (en ISO 27001 en ISO 27701) gecertificeerd is en welke data opslaat binnen de EER waarbij rekening wordt gehouden met de risico's van het kiezen van een niet-Europese aanbieder.

Het uitvoeren van een DPIA zal veel risico's in kaart brengen, waarop vervolgens in het contract of de verwerkersovereenkomst nadere afspraken over kunnen worden gemaakt.

Meerwaarde Zaurus

- Gecertificeerd op informatiebeveiliging (ISO 27001 en NEN 7510), kwaliteit (ISO 9001), privacy (ISO 27701) en bedrijfscontinuïteit (ISO 22301);
- Er is een Chief Information Security Officer (CISO) aangesteld die dagelijks de informatiebeveiliging controleert, toetst en hierover verantwoording over aflegt aan de directie;
- Er is een externe Functionaris Gegevensbescherming aangetrokken om de privacy van betrokkenen te kunnen waarborgen;
- Data worden te allen tijde versleuteld, zowel at rest als in transit. Er is dus sprake van dubbele versleuteling.
- Data blijven te allen tijde binnen de Europese Ruimte (EER).
- Zaurus sluit goede verwerkersovereenkomsten overeenkomstig met de verplichtingen vanuit de AVG en vanuit de ISO 27701.
- Door de implementatie van o.a. de ISO 27001 en de ISO 27701 zijn informatiebeveiliging en privacy ingebed in al onze bedrijfsprocessen. We werken conform privacy by design en privacy by default en werken met gescheiden ontwikkelomgevingen (OTAP).
- De producten en diensten worden frequent gepentest, zowel op ons eigen initiatief als op initiatief van klanten.
- Dagelijks draaien wij vulnerability scans om eventuele ontstane kwetsbaarheden te detecteren en te repareren.

Contacteer Zaurus

Heb je vragen omtrent de informatiebeveiliging of privacy van Zaurus aarzel dan niet om contact op te nemen met onze CISO Michelle Spit via michelle@zaurus.nl.

Kijk voor meer informatie bovendien op:

- Zaurus.nl
- Support.Zaurus.nl
- De Zaurus-pagina op LinkedIn
- Of volg ons op Twitter.

Bibliografie

- Europese Unie (2021, juni 06). Opgehaald van Europese Unie: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679
- AKD benelux laywers . (2020, januari 8). Gaia X – de oplossing voor de US CLOUD Act? Opgehaald van AKD benelux laywers : https://akd.eu/nl/insights/gaia-x-de-oplossing-voor-de-us-cloud-act-
- AP. (2021, juni 6). Data protection impact assessment (DPIA). Opgehaald van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia
- AP. (2021, juni 06). Keuzehulp privacy bij videobel-apps. Opgehaald van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/nieuws/keuzehulp-privacy-bij-videobel-apps
- AP. (2021, juni 06). Zorgverleners en de AVG. Opgehaald van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg#blijft-de-nen-7510-gelden-voor-zorgaanbieders-onder-de-avg-6358
- Brancheorganisaties Zorg. (2021, juni 06). Opgehaald van Brancheorganisaties Zorg: https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/
- CNBC. (2021, April 19). Opgehaald van CNBC: https://www.cnbc.com/2021/04/19/privacy-shield-eu-officials-pushing-hard-for-us-data-sharing-pact.html
- Financieel Dagblad. (2021, juni 07). Toezichthouder maant scholen, universiteiten en Justitie om met Google te stoppen. Financieel Dagblad, p. online.
- GAIA-X. (2021, juni 07). GAIA-X: A Federated Data Infrastructure for Europe. Opgehaald van GAIA-X: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
- ICTRecht. (2019). Advies opslag medische data in de cloud. Amsterdam: ICTRecht.
- ICTRecht. (2021, juni 06). Whatsapp in de gezondheidszorg, gemak voor de zorgverlener of rampzalig voor de privacy? Opgehaald van ICTRecht: https://www.ictrecht.nl/blog/whatsapp-in-de-gezondheidszorg-gemak-voor-de-zorgverlener-of-rampzalig-voor-de-privacy
- KNMG. (2020, maart 31). Beeldbellen tijdens de coronacrisis. Opgehaald van KNMG: https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht-corona/beeldbellen-tijdens-de-coronacrisis.htm
- KNMG. (2021). Omgaan met medische gegevens. Utrecht: KNMG.
- Microsoft. (2021, mei 06). Microsoft. Opgehaald van Op verzoek van Europa: opslag en verwerking van EU-data binnen de EU: https://news.microsoft.com/nl-be/op-verzoek-van-europa-opslag-en-verwerking-van-eu-data-binnen-de-eu/
- NEN. (2021, juni 06). Certificatie en keurmerken NEN 7510. Opgehaald van NEN: https://www.nen.nl/certificatie-en-keurmerken-nen-7510
- Overheid. (2021, juni 06). Opgehaald van Wetten Nederlandse Overheid: https://wetten.overheid.nl/BWBR0005290/2021-05-01/#Boek7_Titeldeel7_Afdeling5_Artikel454
- Rijksoverheid. (2019, oktober 8). Kamerbrief over informatieveiligheid en privacy in de zorg. Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/08/kamerbrief-over-informatieveiligheid-en-privacy-in-de-zorg
- Smarthealth. (2021, juni 06). Smarthealth. Opgehaald van Beeldbeloplossingen: https://smarthealth.live/beeldbellen-zorg/