

DIABASS®

Eén software voor alle meetinstrumenten

Gebruik van oplossingen voor diabetesgegevens- beheer in artsenpraktijk en kliniek



AVG

Belangrijke instructies voor

praktijkhouders/bedrijfsvoering van klinieken

(als verwerkingsverantwoordelijke vlgs. art. 4 nr. 7 AVG)

**functionaris voor gegevensbescherming van
artsenpraktijk en kliniek** (vlgs. art. 37 AVG)



Achtergrond

Systemen voor digitaal diabetesbeheer zijn onontbeerlijk voor een moderne diabetestherapie. Bij het gebruik van dergelijke oplossingen moeten de verantwoordelijken van de praktijk of kliniek er echter op toezien dat de wettelijke verplichtingen (bv. uit de AVG) worden nageleefd, anders bestaat het risico op aanzienlijke boetes en mogelijk zelfs persoonlijke aansprakelijkheid.

Sommige in de markt aangeboden oplossingen overtreden op eclatante wijze de Europese wetgeving; bovendien gebruiken veel aanbieders de patiëntgegevens ook voor eigen commerciële doeleinden.

Het gebruik van dergelijke systemen resulteert dan in aanzienlijke risico's.

Eventuele bedenkingen worden meestal middels verkeerd begrepen of zelfs met de waarheid in strijd zijnde gegevens van de aanbieders gerelativeerd, die artsen kritiekloos vertrouwen. Ook corrumperende toepassingen kunnen de aanschaffingsbeslissing beïnvloeden; daarom worden oplossingen die riskant zijn voor gegevensbescherming vaak ver onder de kosten in de markt voor IT-toepassingen of zelfs volledig gratis aangeboden.

Onze oplossing voor gegevensbeheer **DIABASS®** geniet al bijna 30 (!) jaar het vertrouwen van artsen en patiënten in heel Europa - niet in de laatste plaats ook omdat wij als fabrikant eerlijk communiceren en onze klanten geen onnodige risico's laten lopen.

In deze brochure hebben we daarom uitvoerige informatie bijeen gebracht om een omvangrijke beoordeling met betrekking tot gegevensbescherming bij het gebruik van **DIABASS®** mogelijk te maken.

Informatie over de software

DIABASS®6 PRO (fabrikant: mediaspects GmbH, Friedrichstr. 49, D-72336 Balingen, Duitsland) is lokaal geïnstalleerde en bediende software voor diabetesgegevensbeheer.

Alle met **DIABASS®6 PRO** verzamelde gegevens worden uitsluitend in het lokale netwerk van de praktijk/kliniek verwerkt en opgeslagen. Er worden geen patiëntgegevens aan derden doorgegeven of voor derden toegankelijk gemaakt. Ook telemetrische gegevens (bijvoorbeeld voor onderzoek naar voorgeschreven gedrag) worden niet samengesteld.

Stellingnamen van de autoriteiten die over gegevensbescherming gaan

Voor een toepasselijke beoordeling van gegevensbescherming van oplossingen voor diabetesgegevensbeheer zijn o.a. de volgende stellingnamen van autoriteiten maatgevend:

- "Moet"-lijst van gegevensbescherming die naar de mening van de autoriteit gegevensbescherming dwingend een gegevensbeschermingseffectbeoordeling vlgs. art 35 AVG vereisen.

<https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>

- Stellingname van de Europese autoriteit gegevensbescherming, welke eisen aan de effectiviteit van toestemming o.a. met betrekking tot gezondheidsgegevens te stellen zijn:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf

- Gemeenschappelijke stellingname van de Duitse autoriteit gegevensbescherming betreffende diabetesclouds (in het Duits):

<https://www.diabetologie-online.de/a/datenmanagement-diabetes-clouds-und-datenschutz-dringender-handlungsbedarf-2366301>

Worden met DIABASS® persoonsgebonden resp. naar personen te herleiden gegevens doorgegeven?

Neen, er worden geen patiëntgegevens aan derden doorgegeven of voor derden toegankelijk gemaakt. Ook telemetrische gegevens (bijvoorbeeld voor onderzoek naar voorgeschreven gedrag) worden niet samengesteld.

Alleen in de volgende gevallen worden gegevens doorgegeven:

Update-controle:

Als de automatische updatecontrole geactiveerd is, dan zoekt **DIABASS®6 PRO** via het internet naar een nieuwe programmaversie en biedt deze dan ter installatie aan.

Hiertoe worden de volgende gegevens aan mediaspects doorgegeven, die mogelijk naar personen te herleiden zijn:

IP-adres (noodzakelijk voor iedere internetverbinding), serie-/licentienummer van **DIABASS®**
Daarnaast wordt de volgende technische informatie doorgegeven:

Programmaversie, besturingssysteem, taal evenals de bij de installatie toevallig samengestelde hashtagwaarde

Tip: De updatecontrole is optioneel en kan in de instellingen worden gedeactiveerd.

Instellingen van DIABASS® SecureSend:

Teneinde gegevens via **DIABASS® SecureSend** te kunnen ontvangen, moeten administratieve gegevens van de praktijk/kliniek op een centrale, door mediaspects beheerde server worden opgeslagen en voor patiënten beschikbaar worden gehouden.

Hiervoor is het noodzakelijk dat de volgende administratieve gegevens aan mediaspects worden doorgegeven:

IP-adres (noodzakelijk voor iedere internetverbinding), naam en adres van de praktijk/kliniek, logo van de praktijk/kliniek, e-mailadres van de praktijk/kliniek, statusinformatie (gegevensontvangst toegestaan/niet toegestaan) evenals een optioneel tekstbericht voor alle patiënten (bijv. informatie over praktijkvakantie).

Tip: Het gebruik van **DIABASS® SecureSend** is optioneel en niet dwingend noodzakelijk.

Noodzakelijke vrijgaven:

Voor de updatecontrole resp. het beheer van de instellingen van **DIABASS® SecureSend** moet internettoegang (poorten: 80 resp. 443) op de volgende adressen zijn toegestaan:

[http\(s\)://www.mediaspects.com](http(s)://www.mediaspects.com)

[http\(s\)://www.diabass.com](http(s)://www.diabass.com)

Is voor het gebruik van DIABASS®6 PRO een verwerkersovereenkomst vlgs. art. 28 AVG met mediaspects noodzakelijk?

Nee. mediaspects verwerkt geen persoonsgebonden of aan personen te relateren gegevens voor de praktijk/kliniek. Gegevens worden uitsluitend door de praktijk/kliniek zelf verwerkt en worden ook alleen daar lokaal opgeslagen. Er worden geen patiëntgegevens aan mediaspects of andere derden doorgegeven of toegankelijk gemaakt.

Info: Dat is het verschil met cloudoplossingen

De gebruiksbepalingen van vrijwel alle diabetesclouds vereisen de toestemming van arts/kliniek, zodat de aanbieder de met de cloud verwerkte patiëntgegevens ook voor eigen doeleinden gebruiken mag resp. aan derden doorgeven mag. Sommige van deze aanbieders beweren echter dat de cloud op grond van een geprivilegieerde verwerkersovereenkomst vlgs. art. 28 AVG kan worden gebruikt.

Een echter geen sprake van overeenkomstverwerking wanneer de verwerker de gegevens ook voor eigen doeleinden verwerkt; dit zou dan ontoelaatbaar volgens gegevensverwerking zijn.

Omdergelijkeeigendoeleindenvande verwerker zou het bijvoorbeeld gaan *“als de gegevens bijvoorbeeld voor door hem vastgelegde of mede-gedefinieerde statistische doeleinden, marktonderzoeksdoeleinden, onderzoeksdoeleinden, productoptimalisatiedoeleinden of andere doeleinden verwerkt zouden worden. [...]”* (dit is het standpunt van de Duitse gegevensbeschermingsautoriteiten)



Leidt het gebruik van DDD tot gezamenlijke verantwoordelijkheid (Art 26 GDPR)

Nee. mediaspects verwerkt geen van de persoonsgebonden of aan personen te relateren gegevens die met **DIABASS®6 PRO** worden beheerd. Alle persoonsgebonden of aan personen te relateren gegevens worden uitsluitend verwerkt door de praktijk/kliniek zelf en worden ook alleen daar lokaal opgeslagen. Er worden geen patiëntgegevens aan mediaspects of andere derden doorgegeven of toegankelijk gemaakt.

Info: Dat is het verschil met cloudoplossingen

Als de arts/kliniek de gebruiksbepalingen van een cloudaanbieder accepteren en deze daarmee een via het gebruik van de cloud technisch noodzakelijke gegevensverwerking verregaand eigen gebruik van de patiëntgegevens mogelijk wil maken, bestaat in zoverre in de regel een gemeenschappelijke verantwoordelijkheid met de aanbieder vlgs. art. 26 AVG.

De te regelen verantwoordelijkheid van arts/kliniek bestaat er dan primair uit aan de aanbieder een commercieel gebruik van de gegevens mogelijk te maken. Een geloofwaardige medische noodzaak voor een dergelijke verwerking is moeilijk voorstelbaar. Dergelijke samenwerking tussen artsen en aanbieders van producten onder de verordening zouden zowel strafrechtelijk als ook beroepsrechtelijk niet onproblematisch zijn.



Is voor de verwerking van gezondheidsgegevens met **DIABASS®6 PRO** een aparte resp. uitdrukkelijke toestemming van de patiënt vlgs. art. 9 par. 2 lit a) AVG noodzakelijk?

Nee. De samenstelling en verwerking van deze gegevens vindt plaats ter vervulling van juridische verplichtingen van arts/kliniek resp. ter vervulling van de behandelingsovereenkomst.

Vlgs. art. 9 par. 2 lit h) AVG is daarom geen uitdrukkelijke toestemming vereist.

Info: Dat is het verschil met cloudoplossingen

De aldaar vermelde gebruikersbepalingen vereisten meestal de toestemming dat de cloudaanbieder de aldaar verwerkte patiëntgegevens ook voor eigen doeleinden mag gebruiken resp. aan derden mag doorgeven. Een dergelijk vergaande gegevensverwerking is medisch resp. ter behandeling echter niet “noodzakelijk” in de zin van art. 9 par. 2 lit h) AVG.

Hiertoe is de uitdrukkelijke toestemming van iedere individuele patiënt nodig. Deze is echter uitsluitend effectief als de patiënt van tevoren uitgebreid is ingelicht en hij een echte keuzevrijheid heeft gehad.

Daaraan verandert ook niets als de patiënt zijn gegevens zelf in de cloud instelt:

De praktijk/kliniek is vlgs. art. 4 nr. 7 AVG desalniettemin de verwerkingsverantwoordelijke met betrekking tot gegevensbescherming, omdat alleen zij beslist of een door een patiënt beschikbaar gemaakte cloudtoegang als middel voor gegevensverwerking voor de behandeling gebruikt moet worden.

Een dergelijk cloudgebruik zou dan ook niet “passief” zijn, zoals sommige aanbieders dat beweren: De behandelende persoon bepaalt bijvoorbeeld door het geven van het “inloggen” de tijdsruimte van zijn inzage evenals aard en omvang van de opgevraagde analyse, ook zelfs eventuele gegevens, die onderhevig zijn aan het ambtsgeheim van een arts. De praktijk/kliniek draagt dusdoende het volledige risico of een van de patiënt verkregen “clouduitnodiging” daadwerkelijk een uitdrukkelijke, geïnformeerde en zelf bepaalde toestemming behelst. Daarvan kan echter alleen worden uitgegaan als de patiënt uitgebreid werd ingelicht en hem van de kant van de praktijk/kliniek ook een gegevensbeperkend alternatief voor de overdracht resp. verwerking van zijn gegevens is aangeboden.

Moet **DIABASS®** in de register van de verwerkingsactiviteiten (art. 30 AVG) worden opgenomen?

Ja. Praktijk/kliniek zijn verplicht alle verwerkingsactiviteiten vlgs. art. 30 AVG te documenteren. Alleszins is dit met weinig moeite te regelen, omdat bij **DIABASS®** slechts weinig informatie vereist is. Op aanvraag stellen wij graag een gratis model ter beschikking.

Info: Dat is het verschil met cloudoplossingen

De gebruiksbepalingen van alle gangbare diabetesclouds zijn zeer complex en omvangrijk. Arts/kliniek moeten daar een veelvoud aan gegevensverwerkingsstappen voltooien die in veel gevallen ook ver boven de medisch noodzakelijke doeleinden uit reiken. Alle gebruiksbepalingen evenals documenten die als eveneens geldig zijn aangemerkt moeten dan zorgvuldig worden gecontroleerd en alle daar geregelde gegevensverwerkingsstappen vlgs. art. 30 AVG moeten in de register worden opgenomen. De catalogus mag inhoudelijk niet in tegenspraak zijn met de gebruiksbepalingen.

Moet voor **DIABASS®** een gegevensbeschermingseffectbeoordeling vlgs. art. 35 AVG worden gemaakt?

Een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd als de verwerking een hoog risico voor de rechten en vrijheden van natuurlijke personen tot gevolg heeft (art. 35 AVG).

Hiervan kan men bij **DIABASS®** niet uitgaan, omdat alle gegevens uitsluitend op het lokale netwerk van de praktijk/kliniek worden verwerkt en uitsluitend bewezen technologieën worden gehanteerd.

Het gebruik van **DIABASS®** kan daarom worden vergeleken met andere lokale software, die in het kader van de behandeling wordt gebruikt, bijvoorbeeld Word voor het schrijven van een doktersattest of lokaal geïnstalleerde praktijkbeheerssoftware.

Info: Dat is het verschil met cloudoplossingen

De autoriteit gegevensbeheer heeft een lijst met gegevensverwerking gepubliceerd, die dwingend een inschatting van de gevolgen van gegevensverwerking vlgs. art. 35 AVG vereist.

<https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>

De meeste diabetesclouds moeten tenminste aan een van de in deze lijst als voorbeeld genoemde verwerkingsmethoden voldoen, in het bijzonder Nr. 7, 14 en 17.

Daarnaast gaan de gebruiksbepalingen van veel diabetesclouds er van uit dat de cloudaanbieder de aldaar verwerkte patiëntgegevens ook voor eigen doeleinden mag gebruiken resp. aan derden mag doorgeven. Alleen al om deze reden kan men daar uitgaan van een hoog risico voor de rechten van patiënten.



Waarop moet worden gelet bij het gebruik van **DIABASS® SecureSend**?

DIABASS® SecureSend dient voor de veilige overdracht van gegevens door de patiënt.

De gegevens worden lokaal op de PC resp. smartphone van de patiënt streng beveiligd “end-to-end” versleuteld (AES-256) en vervolgens per e-mail aan de praktijk/kliniek doorgegeven. Afhankelijk van de lokale instellingen bij de ontvanger worden de gegevens dan automatisch of door dubbel te klikken door de gebruiker van het programma ontsleuteld en in het gegevensbestand van **DIABASS®** ingevoerd.

Alleen de patiënt bepaalt of hij de mail met de versleutelde gegevens via zijn eigen e-mailprogramma wil versturen of dat hij het aanbieden ter verzending via de door mediaspects beheerde server wil gebruiken. In het laatste geval worden de versleutelde gegevens per e-mail en met een neutraal afzender-adres aan de ontvanger doorgegeven. Deze versleutelde gegevens kunnen daarbij noch door mediaspects noch door derden worden ingezien, de versleutelingsinformatie is alleen bij de patiënt en de ontvanger bekend.

Info: Dat is het verschil met cloudoplossingen

Bij een gegevensoverdracht met gebruikmaking van cloud-oplossingen vindt regelmatig geen end-to-end versleuteling plaats, doch slechts een transport-versleuteling. De gezondheidsgegevens worden daarom aan de cloud-aanbieder toegankelijk gemaakt. Bovendien moeten patiënt en arts bijna altijd akkoord gaan met het commerciële gebruik van de gegevens door de aanbieder resp. met de overdracht van de gegevens aan derden, anders kan de cloud zelfs helemaal niet worden gebruikt.



Herbergt het gebruik van DIABASS® het risico in zich dat voor arts-/diabetesraadpleging gegevens over hun verordeninggedrag, voor de behandelkwaliteit of voor hun gebruiksgedrag verzameld en waar mogelijk door derden beoordeeld en gedocumenteerd worden?

Nee. Dergelijke gegevens over het gebruiksgedrag worden door DIABASS® niet samengesteld. Alle bij het gebruik van DIABASS® ontstane gegevens worden uitsluitend lokaal opgeslagen en zijn niet toegankelijk voor derden.



Info: Dat is het verschil met cloudoplossingen

De gebruiksbepalingen van de meeste cloudoplossingen voorzien erin dat dergelijke gebruiks- en kwaliteitsgegevens uitgebreid door de gebruiker mogen worden gebruikt en/of aan derden mogen worden doorgegeven. Maar ook sommige lokaal functionerende diabetesbeheersoftware geeft telemetrie- en gebruiksgegevens door aan de fabrikant, zonder dat de gebruiker hierover waarneembaar wordt geïnformeerd.



Zijn cloud-oplossingen niet beter dan lokale oplossingen?

In publicaties of tijdens voordrachtbijeenkomsten wordt graag beweerd dat een “cloud” gewenst is resp. optimaal zou zijn voor het diabetesgegevensbeheer van de arts. Zeer vaak gaat het daarbij echter alleen om reclame-uitingen, die niet opgewassen zijn tegen kritische vragen.

Hieronder een paar voorbeelden

Bewering ...	... en werkelijkheid
De cloud heeft het voordeel dat de patiënt de gegevens zelf instelt en dat het diabetesteam altijd actuele waarden kan gebruiken, men bespaart zich de moeite van gegevensoverdracht	Hiervoor is geen cloud noodzakelijk. Met de voor tele-medische functies geschikte lokale software zoals DIABASS® kan dezelfde functionaliteit worden behaald – en dit zonder de met een cloud verbonden risico's (bijvoorbeeld: risico op boetegeld bij ongeoorloofde doorgave van gegevens, een toegang tot gegevens zonder internetverbinding, verstoorde bereikbaarheid/beschikbaarheid van de cloud, ...).
Bij een cloud hoeft men niets te installeren	Bij bijna alle diabetesclouds moet een zgn. uploader worden geïnstalleerd. Bovendien moet ook de firewall worden geopend om de cloudtoegang mogelijk te maken – met alle gevolgen voor de IT-veiligheid van de praktijk/kliniek.
De cloud bespaart opslagruimte omdat de patiëntgegevens extern worden opgeslagen	Dat is weliswaar juist maar zou feitelijk echter nauwelijks een rol spelen: zelfs omvangrijke gegevensbestanden (CGM en insulinepomp) van duizenden patiënten via de voorgeschreven minimale opslagtijd (10 jaar) kunnen moeiteloos op een in de handel verkrijgbare USB-stick worden opgeslagen.
De cloud is gratis resp. goedkoper dan het aanschaffen van lokale software	Met betrekking tot de pure aanschaffkosten kan dit bij cloud-oplossingen van toepassing zijn, die tegen een onrealistisch lage, gecorrumpeerde prijs worden aangeboden. De aannahme van dergelijke toepassingen resp. gunstige voordelen herbergt alleszins strafrechtelijke en belastingtechnische risico's in zich. Naast de pure aankoop prijs moeten echter ook de aanzienlijke bijkomende kosten in aanmerking worden genomen, die bij het rechtmatige gebruik van een cloud-oplossing dwingend optreden. Aan de noodzakelijke juridische controle van de meest complexe gebruiksbepalingen en de doorvoering van een voorgeschreven gegevensbeschermingseffectbeoordeling zijn aanzienlijke kosten verbonden. Ook de noodzakelijke personele bezetting voor patiëntvoorlichting, voor het verkrijgen van effectieve toestemming evenals het blijvend voldoen aan wettelijk voorgeschreven, administratieve plichten omtrent gegevensbescherming zijn aanzienlijk.
"Onze cloud is juridisch gecontroleerd en alles is toegestaan"	Een door een praktijk/kliniek zelf doorgevoerde juridische controle zal vaak wel tot een ander resultaat leiden. Bovendien moeten de arts/ kliniek zich in "de kleine lettertjes" meestal verplichten de uitsluitende verantwoording te nemen voor de juridische toelaatbaarheid van het cloudgebruik.
"De gegevensbescherming van onze cloud is gecertificeerd; de server staat in Duitsland resp. de EU"	Dit feit alleen maakt het cloudgebruik niet toelaatbaar of zonder problemen. De serverlocatie in Europa voorkomt slechts de aanvullende problemen, die bij gegevensoverdracht naar derde landen komt kijken. En de certificering van de aanbieder speelt bij de eigen verantwoordelijkheid van praktijk/kliniek geen rol.

DIABASS®

Eén software voor alle meetinstrumenten

NADERE INFORMATIE

www.diabass.com



Beratungsgesellschaft
für neue Medien mbH
Postbus 10 07 31
D-72307 Balingen, Duitsland

Tel.: +49 (0) 7433 96 75 970
Fax: +49 (0) 7433 96 75 971
E-mail: info@mediaspects.de
Internet: www.mediaspects.de



Wij zijn gecertificeerd volgens
DIN ISO 13485
www.tuev-sued.de/ps-zert