

BVKD e. V. · Kirchberg 21 · 37431 Bad Lauterberg im Harz

Anrede  
Vorname Name  
Straße Nr.  
PLZ Ort

Bundes-Geschäftsstelle  
Kirchberg 21  
37431 Bad Lauterberg

Telefon 05524 / 81 218  
Telefax 05524 / 81 398

info@die-diabetes-kliniken.de  
www.die-diabetes-kliniken.de

Bad Lauterberg, 5. März 2021

### Fragen zu datenschutzrechtlichen Bedingungen

Sehr geehrte ...,

der Bundesverband Klinischer Diabetes-Einrichtungen – Die Diabetes- Kliniken e.V. - vertritt die Interessen von etwa 120 auf die Behandlung von Diabetes mellitus spezialisierten Kliniken.

Unsere Mitgliedshäuser müssen selbstverständlich alle in Deutschland geltenden Vorschriften zu Themen des Datenschutzes und der Datensicherheit umsetzen. Bei der Nutzung von Daten, die von Blutzuckermessgeräten bzw. –sensoren und Insulinpumpen erhoben und im Krankenhaus verarbeitet werden, ist unserem Verband derzeit nicht klar, inwieweit die Datenspeicherung in cloudbasierten Systemen den aktuellen Rechtsgrundlagen entspricht.

Wir möchten im Interesse unserer Mitglieder deshalb gern von Ihnen wissen:

1. Auf welcher Rechtsgrundlage erfolgen die zur Nutzung der von Medtronic angebotenen Cloud-Lösung (im Folgenden: „Produkt“) erforderlichen Datenverarbeitungsvorgänge?
2. Erfolgt die Datenverarbeitung ausschließlich innerhalb der EU?
3. Ist für die mit der Nutzung des Produkts verbundenen Datenübermittlungs- und Verarbeitungsvorgänge eine Einwilligung der Patienten erforderlich?
4. Ist die die Nutzung Ihrer Cloud-Lösung auf Basis eines Auftragsverarbeitungsvertrags (gem. Art. 28 DSGVO) rechtlich unproblematisch möglich?
5. Werden mit dem Produkt verwaltete Patientendaten und/oder hieraus abgeleitete oder anonymisierte Daten von Ihnen oder Dritten ganz oder teilweise auch für eigene Zwecke genutzt, beispielsweise zu statistischen Zwecken, zur Produktverbesserung oder Forschung? Falls ja, bitte angeben, welche Daten von wem in welcher Form und für welche Zwecke verarbeitet werden.

**Vorstand:** Dr. med. Thomas Werner (1. Vorsitzender) · Dr. med. Karin Overlack (2. Vorsitzende) · Dipl.-BW Klaus-Dieter Wilde (Schatzmeister) · Prof. Dr. med. Wolfgang Motz (Pressesprecher) · Birgit Friedrich (Schriftführerin) · Dr. Christian Graf (Beisitzer) · Prof. Dr. med. Matthias Weck (Beisitzer)

**Vereinsregister:** Amtsgericht Hamburg · VR 16924

**Bankverbindung:** IBAN: DE76 4725 1550 0001 0052 97 · Sparkasse Hörter

6 Welche datenschutzrechtlichen Organisationsmaßnahmen muss der Anwender in Bezug auf das Produkt vornehmen, damit das Produkt datenschutzkonform eingesetzt werden kann?

7. Wie ist garantiert, dass die mit dem Produkt verwalteten Daten für die Dauer der jeweils geltenden gesetzlich vorgeschriebenen Aufbewahrungsfristen zugänglich sind?

8. Ist für die Nutzung des Produkts die dauerhafte Einwilligung des Anwenders und/oder des jeweiligen Patienten in Nutzungsbestimmungen erforderlich? Falls ja: bitte senden Sie uns die aktuelle Fassung der Nutzungsbedingungen

9 Welche Kosten fallen für die Nutzung des Produktes an?

10. Ist die komplette Nutzung des Produkts ohne Installation, d.h. allein per Internet-Browser möglich oder müssen zusätzlich Komponenten wie Treiber, Uploadprogramme oder Dienste lokal installiert werden? Falls eine Installation erforderlich ist: was genau muss installiert werden und welche administrativen Rechte sind dazu erforderlich? Können sich hierdurch Risiken in Bezug auf die IT-Sicherheit der Klinik ergeben?

Über eine zeitnahe Beantwortung unserer Fragen würden wir uns freuen. Je ausführlicher Sie antworten, desto besser können die Datenschutzbeauftragten unserer Mitglieder die mit dem Produkt einhergehenden Datenverarbeitungsvorgänge einschätzen

Für Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

Klaus-Dieter Jannasch  
Geschäftsstellenleiter

# Angefragte Unternehmen

Medtronic

Dexcom

Abbott

Roche

Ascensia

Menarini

Ypsomed

Insulet

VitalAire/Tandem

Medtrum

Sooil/IME-DE

SINOVO

# Antwortschreiben der angefragten Unternehmen

Von folgenden Unternehmen liegen Antwortschreiben vor

1. Medtronic
2. Dexcom
3. Roche
4. Menarini
5. Ypsomed
6. VitalAire/Tandem
7. Sooil/IME-DE

Medtronic GmbH · Postfach 1441 · 40639 Meerbusch

Bundesverband Klinischer Diabetes-Einrichtungen e.V.  
Herrn Klaus-Dieter Jannaschk  
Kirchberg 21  
37431 Bad Lauterberg

Ihre Anfrage zu datenschutzrechtlichen Bedingungen

16. April 2021

Sehr geehrter Herr Jannaschk,

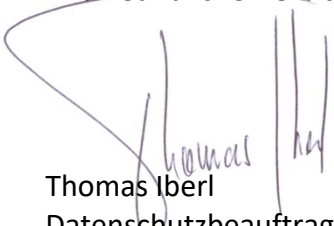
haben Sie vielen Dank für Ihre Anfrage vom 05.03.2021.

Üblicherweise beantworten wir Fragen unserer Kunden zu datenschutzrechtlichen Bedingungen produktspezifisch im konkreten Einzelfalle direkt gegenüber diesen Kunden und bitten um Verständnis, dass wir auch in diesem Fall von dieser Praxis nicht abweichen.

Allgemein können wir Ihnen mitteilen, dass von uns angebotene Softwarelösungen die Patientendaten für die jeweilige Anwendung in der EU - bzw. bei Patienten in der EU oder Kunden in der EU - auch grds., d.h. im Regelbetrieb, in der EU verarbeiten. Dies beinhaltet ebenso die Organisation der Systeme wie auch die notwendige Kommunikationsinfrastruktur.

Unsere Produkte sind selbstverständlich auch unter Datenschutzgesichtspunkten intensiv geprüft und durchlaufen eine Risikoanalyse und Risikobeurteilung, so dass diese die gesetzlichen Voraussetzungen erfüllen. So erfolgt die Prüfung u.a. nach den gesetzlichen Bestimmungen und Regeln speziell für Gesundheitsdaten, bevor die Produkte in den Markt gebracht werden.

Mit freundlichen Grüßen

  
Thomas Iberl  
Datenschutzbeauftragter für  
Medtronic GmbH

Dexcom Deutschland GmbH, Haifa-Allee 2, D-55128 Mainz

## Antworten auf Fragen des Bundesverbandes Klinischer Diabetes-Einrichtungen e. V (BVKD e.V.)

### 1. Auf welcher Rechtsgrundlage erfolgen die zur Nutzung der von Ihnen angebotenen Cloud-Lösung (im Folgenden: „Produkt“) erforderlichen Datenverarbeitungsvorgänge?

Um Ihnen umfassende Antworten auf Ihre Fragen insbesondere zu den Datenverarbeitungstätigkeiten durch das Dexcom G6 CGM-System geben zu können, möchten wir Ihnen zunächst einen Überblick über unser Dexcom CGM-System geben (siehe unten unter 1.1)). Darauf aufbauend informieren wir Sie über die Rechtsgrundlagen für die unter 1.1) beschriebenen Verarbeitungstätigkeiten (siehe unten unter Ziff. 1.2)):

#### 1.1) Übersicht über das Dexcom CGM-System

Das Dexcom G6 CGM-System ist ein Gerät für das persönliche Glukosemanagement von Personen mit Diabetes. Das G6 CGM-System ermöglicht es Gesundheitsdienstleistern ("HCPs"), wie z. B. Krankenhäusern, die Glukosewerte von Patienten einzusehen.

Das G6 CGM-System besteht aus einem subkutanen Sensor, der mit einem Pflaster am Patienten angebracht wird, einem Sender, der Glukosewerte über Bluetooth (BLE) sendet, und einem Empfänger, der die Übertragungen erfasst und die Glukosewerte anzeigt. Dexcom bietet verschiedene Konfigurationen mit einer Reihe von optionalen Funktionen zur Verarbeitung und Anzeige der Daten an.

#### Komponenten des CGM-Systems:

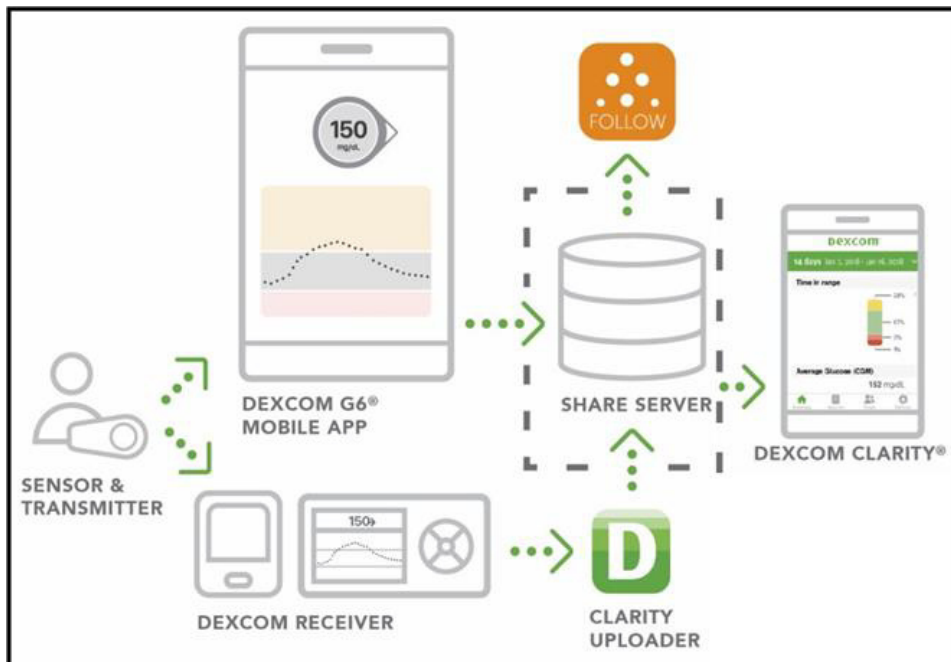
- **Applikator** - Mit einem einfachen One-Touch-Applikator wird ein kleiner Sensor direkt unter die Haut des Patienten eingeführt.
- **Sensor/Transmitter-Kombination** - Ein schlanker Sensor misst kontinuierlich den Glukosespiegel unter der Haut. Er wird mit einem Pflaster für bis zu 10 Tage an dem Patienten angebracht und sendet die Daten drahtlos über einen Bluetooth-Sender an ein Anzeigegerät/Empfänger. Der Bluetooth-Sender kann nach entsprechender Reinigung für denselben Patienten wiederverwendet werden, wenn dessen Aufenthalt länger als 10 Tage dauert.
- **Empfänger** - Ein Gerät, das Daten über Bluetooth vom Sender empfängt und Glukosewerte anzeigt, die alle 5 Minuten aktualisiert werden. Der Empfänger muss sich in unmittelbarer Reichweite (20 Fuß ohne Hindernisse) des vom Patienten getragenen Senders befinden. Das G6 CGM-System unterstützt einen dedizierten Dexcom-Empfänger oder eines von mehreren kompatiblen Smart Devices. Der dedizierte Empfänger ist nur in der Lage, die CGM-Daten der letzten 24 Stunden anzuzeigen.
- **Apps**
  - **G6** ist eine mobile App, die auf einem unterstützten BLE-fähigen Smart Device installiert werden muss, um Glukosewerte vom G6-Sender zu empfangen.

- **Clarity** ist eine optionale webbasierte Anwendung, mit der HCPs historische CGM-Daten überprüfen, analysieren und Berichte erstellen können. Clarity ist nicht in das System der elektronischen Patientenakte oder vergleichbaren Datenbanken zur Aufbewahrung von Patientendaten integriert. Die Berichte können ausgedruckt und gescannt/hochgeladen werden, um sie manuell zu derartigen elektronischen Patientenakten hinzuzufügen.
- **Follow** ist eine optionale mobile App, mit der Patienten ihre CGM-Daten mit Familie, Freunden und Betreuern teilen können. Dies ermöglicht die Fernüberwachung eines Patienten von zusätzlichen Geräten aus.
- Die **Datenplattform** von Dexcom wird auf der Google Cloud Platform (GCP) gehostet. Innerhalb von GCP werden die Daten auf regionsspezifischen Servern verarbeitet und gespeichert (europäische Daten werden innerhalb der EU gespeichert), wobei eine belastbare, fehlertolerante Architektur zum Einsatz kommt.

## System-Konfigurationen

Die oben näher beschriebene G6-Sensor/Transmitter-Kombination ist für alle System-Konfigurationen erforderlich. Dies ist der vom Patienten getragene Transmitter, der die Glukosewerte misst und die Daten über Bluetooth überträgt.

Von dort aus bietet Dexcom zwei Konfigurationen (lokal und drahtlos, unten beschrieben) im Krankenhausumfeld an, um das Glukosemanagement des Patienten zu unterstützen. Beide Konfigurationen ermöglichen es dem medizinischen Personal, den Blutzucker des Patienten zu überwachen, ohne das Patientenzimmer zu betreten. Außerdem werden von den Dexcom-Geräten nur die Glukosewerte des Patienten erfasst; es werden keine anderen Krankenhaus-/Patienteninformationen erfasst. Beide Konfigurationen zeichnen außer den CGM-Daten keine direkten personenbezogenen Daten des Patienten auf (z. B. Name, Geburtsdatum, Patienten-ID usw.).



Bei der **lokalen Konfiguration** wird ein dedizierter Dexcom-Empfänger oder ein Smart Device zum Empfang der über die BLE-Funktion gesendeten Blutzuckerwerte (die übrigen drahtlosen Funktionen außerhalb der BLE-Funktion wie W-LAN bleiben dabei deaktiviert) verwendet, um den Blutzucker des Patienten alle 5 Minuten anzuzeigen. Das Empfangsgerät ist die einzige Echtzeitanzeige, die in dieser Konfiguration verfügbar ist. Die lokale Konfiguration ermöglicht es,

Patientenglukosewerte nicht mit Dexcom-Systemen zu teilen, ist jedoch nicht mit der Fernüberwachungs-App Follow kompatibel.

- Retrospektive Überprüfung und Berichte: Dexcom Clarity kann mit dem dedizierten Empfänger verwendet werden. Es erfordert jedoch die Installation des Clarity Uploader-Tools auf mindestens einem Krankenhaus-Desktop/Laptop. Der dedizierte Empfänger muss dann über USB an den Desktop/Laptop angeschlossen werden, damit die Glukosedaten des Patienten manuell in die Clarity-Webanwendung hochgeladen werden können, die einen Internetzugang erfordert. Durch das Hochladen werden die Blutzuckerwerte des Patienten an die Dexcom-Cloud gesendet, aber die Frequenz des Datenaustauschs ist begrenzt (aufgrund des manuellen Hochladens) und das Telefon, das als Empfänger dient, muss keinen Internetzugang haben.

Die **drahtlose Konfiguration** wird für die Dateneingabe durch Kliniken eingesetzt, um das Clarity Clinic Konto einzurichten, oder wenn auf die Daten über ein verknüpftes Patientenkonto zugegriffen wird. Sie erfordert ein kompatibles Smart Device. Auf jedem Smart Device muss die Dexcom G6 App installiert sein, und es ist ein Internetzugang entweder über einen mobilen Datentarif oder über WLAN erforderlich, um die Glukosewerte des Patienten an die Datenplattform von Dexcom zu senden. Dies ermöglicht die Fernüberwachung und die retrospektive Datenanalyse mit Clarity, ohne dass manuelle Uploads erforderlich sind.

- Retrospektive Überprüfung und Berichte: Dexcom Clarity kann nahtlos mit der drahtlosen Konfiguration verwendet werden, da die Installation der Desktop-Software und manuelle Uploads nicht erforderlich sind. Die angezeigten Glukosedaten in Clarity können im Vergleich zur Echtzeitanzeige um mehrere Stunden nachhinken. Solange kein Verbindungsverlust auf dem Smart Device, entweder zwischen Empfänger und Sender oder zwischen Empfänger und Internet, größer als 3 Stunden auftritt, werden alle Glukosewerte weiterhin aufgezeichnet und sind schließlich in Clarity sichtbar.
- Fernüberwachung: Die Dexcom Follow App kann bei einer stabilen Internetverbindung die Glukosewerte von bis zu 10 Patienten, die das G6 CGM tragen, in Echtzeit auf einem einzigen Smart Device anzeigen. Ebenso kann ein einzelner Patient von bis zu 10 Personen verfolgt werden. Dies ermöglicht es dem medizinischen Personal, ihre Patienten zu überwachen, einschließlich Warnungen und Alarmer, ohne sich physisch zum Display in der Nähe des Patienten zu begeben, wie es die lokale Konfiguration erfordert. Die Verfolgung wird nur auf Einladung des Smart Device aktiviert, das Daten direkt vom Sender des Patienten empfängt und mit dem anonymen, von Dexcom bereitgestellten Konto verbunden ist.

## 1.2) Beziehung zwischen Dexcom und HCPs und Rechtsgrundlagen für die Verarbeitungstätigkeiten

Wir möchten Ihnen näher erläutern, wie wir das Dexcom CGM-System im Hinblick auf das Datenschutzrecht und insbesondere die Datenschutz-Grundverordnung ("**DSGVO**") eingerichtet haben.

Um es zusammenzufassen, in den obigen Szenarien der lokalen und drahtlosen Konfiguration verarbeitet Dexcom (personenbezogene) Daten als Auftragsverarbeiter für HCPs wie Kliniken, die Patientendaten in ein Clarity-Klinikkonto eingeben, um dieses damit einzurichten (in Bezug auf die personenbezogenen Daten der administrierenden Klinikmitarbeiter, wie Name und Funktion, nicht aber in Bezug auf Patientendaten wie z.B. Glukosedaten der Patienten) (drahtlose Konfiguration), und insoweit (Glukose-)Daten von Patientenempfängern über das Klinikkonto auf Dexcom Clarity hochgeladen wurden, und keine anderen Dexcom-Dienste vom Patienten in Anspruch genommen werden (lokale Konfiguration).

Nichtsdestotrotz verarbeitet Dexcom auch Daten als Verantwortlicher, wenn Dexcom personenbezogene Daten direkt von Patienten durch die Nutzung von Dexcom-Diensten, einschließlich Dexcom Clarity, erhält. In diesen Fällen gestattet es der Patient Dexcom, dass seine personenbezogenen Daten in der Cloud mit Dexcom gemäß der Datenschutzrichtlinie und den



Nutzungsbedingungen von Dexcom geteilt werden.

Dazu weitere Details:

### **1.2.1) Dexcom als Auftragsverarbeiter für Krankenhäuser und Rechtsgrundlagen**

Dexcom verarbeitet Patientendaten über Clarity als Auftragsverarbeiter für Krankenhäuser, wenn das Krankenhaus in Verbindung mit einem Clarity-Klinikkonto über ein speziell mit diesem verknüpftes Patientenkonto auf die Patientendaten zugreift, und wenn die Daten von einem Patienten über einen Dexcom-Empfänger im Konto des Krankenhauses auf Dexcom Clarity hochgeladen werden, d.h. wenn keine anderen Dexcom-Dienste (wie z.B. die Dexcom-App) vom Patienten genutzt werden oder wurden.

In diesem Szenario bietet Dexcom eine Standard-Auftragsverarbeitungsvereinbarung zum Abschluss mit HCPs an.

Hinsichtlich der Rechtsgrundlage ist es grundsätzlich die Aufgabe der HCPs als Verantwortliche, die Rechtmäßigkeit der Datenverarbeitung sicherzustellen und (falls sie dies für erforderlich halten) eine etwaige Einwilligung der Patienten rechtskonform einzuholen.

Die DSGVO sieht in Art. 9 viele Ausnahmen vor, unter denen Gesundheitsdaten rechtmäßig verarbeitet werden dürfen. Insbesondere Art. 9(2)(h) DSGVO bietet eine Vielzahl von Möglichkeiten im Gesundheitsbereich, bei denen eine Einwilligung nicht erforderlich ist und Daten ohne Einwilligung der Patienten verarbeitet werden können. Unseres Erachtens können viele Verarbeitungsaktivitäten von HCPs durch Art. 9(2)(h) DSGVO gerechtfertigt werden.

Das Vorliegen einer solchen Ausnahme nach Art. 9 DSGVO sollte jedoch - wie üblich - von dem für die konkrete Verarbeitungstätigkeit verantwortlichen HCP beurteilt werden. Letztlich ist Dexcom auch nicht befugt, Rechtsberatung zu diesem Thema zu leisten (dies verbietet das *Gesetz über außergerichtliche Rechtsdienstleistungen* in Deutschland).

### **1.2.2) Dexcom als Verantwortlicher in Bezug auf HCPs und Rechtsgrundlagen**

Dexcom kann hingegen in bestimmten Szenarien gegenüber den Patienten als datenschutzrechtlich Verantwortlicher eingestuft werden. Dexcom verarbeitet personenbezogene Daten als für die Verarbeitung Verantwortlicher in dem Umfang, in dem Dexcom personenbezogene Daten direkt von Patienten durch die Nutzung der Dexcom-Dienste, einschließlich Dexcom Clarity, erhält, wobei der Patient Dexcom durch die Akzeptanz der Dexcom-Nutzungsbedingungen und Datenschutzrichtlinie zustimmt, seine Patientendaten mit Dexcom in Übereinstimmung damit zu teilen.

In diesen Fällen können die Patienten einem HCP über die Dexcom Services gezielt Zugang zu bestimmten Patientendaten gewähren. Dies führt nicht dazu, dass sich Dexcom als Auftragsverarbeiter in Bezug auf die HCPs qualifiziert. In diesen Fällen werden die HCPs lediglich speziell vom Patienten autorisiert, auf Patientendaten zuzugreifen. Diese Patienten können frei entscheiden, Dexcom anzuweisen, Patientendaten an so genannte *Designated Recipients* wie HCPs weiterzugeben (siehe hierzu auch unsere Datenschutzrichtlinie unter dem Abschnitt "Wie wir gesammelte persönliche Daten weitergeben"). Die bloße Gewährung des Zugriffs auf personenbezogene Daten durch den Patienten stellt keine Verarbeitung durch Dexcom im Auftrag von HCPs dar. Ein Auftragsverarbeitungsvertrag ist daher in solchen Fällen nicht erforderlich.

In Fällen, in denen Dexcom der für die Verarbeitung Verantwortliche ist, holt Dexcom Einwilligungen für die Datenverarbeitungstätigkeiten ein (z. B. über die Dexcom-App) und Patienten können in jedem Einzelfall den Zugriff von HCPs auf Patientendaten über die App genehmigen (was eine Einwilligung gemäß DSGVO darstellt). Der Patient kann die Weitergabe an HCPs natürlich jederzeit starten oder beenden (siehe Details zu dieser Einwilligung unter Punkt 3) unten).

## **2. Erfolgt die Datenverarbeitung ausschließlich innerhalb der EU?**

Personenbezogene Daten von Patienten und medizinischem Fachpersonal aus der EU, dem EWR, Großbritannien und der Schweiz werden in der EU auf sicheren, zertifizierten Servern gespeichert. Deutsche Patientendaten werden in Frankfurt, Deutschland, gespeichert. Ein Zugriff von außerhalb der EU erfolgt nur unter eingeschränkten Umständen, die nach der DSGVO und europäischem Recht legitim sind, wie z. B. Einwilligung, Verwendung für vertragliche Zwecke oder legitime

Forschung und Entwicklung in pseudonymisierter, aggregierter und/oder anonymisierter Form oder zur Erfüllung regulatorischer Anforderungen im Gesundheitswesen, um die Sicherheit unserer Produkte zu gewährleisten. Solche Übermittlungen beruhen rechtlich auf den in der DSGVO vorgesehenen Mitteln (insbesondere den Standardvertragsklauseln) und entsprechen den Anforderungen des Schrems II-Urteils des Europäischen Gerichtshofs.

### **3. Ist für die mit der Nutzung des Produkts verbundenen Datenübermittlungs- und Verarbeitungsvorgänge eine Einwilligung der Patienten erforderlich?**

In Fällen, in denen Dexcom der für die Verarbeitung Verantwortliche ist (siehe oben), holt Dexcom eine solche Einwilligung von den Patienten für die im Folgenden beschriebenen Zwecke ein. Um es noch einmal zu wiederholen: Die HCPs spielen in diesem Szenario aus datenschutzrechtlicher Sicht keine Rolle, da die Patienten den HCPs über die Dexcom-Dienste nur als sogenannte *Designated Recipients* gezielt Zugriff auf bestimmte Patientendaten gewähren (es sei denn, HCPs verarbeiten Patientendaten in Verbindung mit einem Clarity-Klinikkonto, bei dem die Daten von einem Patienten über einen Dexcom-Empfänger im Konto der Klinik auf Dexcom Clarity hochgeladen werden, d. h. wenn keine anderen Dexcom-Dienste (wie die Dexcom-App) vom Patienten genutzt werden oder wurden).

Die Zustimmung wird von Dexcom für die folgenden Zwecke eingeholt:

- Senden von Patientendaten an Dexcom, was die folgenden Optionen ermöglicht:
  - Teilen der Daten mit Followern,
  - Verwenden der Dexcom Clarity Software,
  - Speichern der Alarme und andere App-Einstellungen für das Smart Device.
- Verwenden der Dexcom Clarity Software: Clarity ist ein retrospektives Therapiemanagement-Tool, mit dem Patienten auf alle ihre historischen Blutzuckermessungen zugreifen können.
- Aktivieren von auf Wunsch erweiterter technischer Supportleistungen: Wenn Patienten Probleme mit ihrem CGM-System haben, können die Mitarbeiter des technischen Supports von Dexcom auf die Gesundheitsdaten des Patienten zugreifen, um die Probleme zu beheben oder Fragen zu beantworten. Die Mitarbeiter des technischen Supports haben nur auf ausdrücklichen Wunsch des Patienten Zugriff auf die Daten.

Wenn Dexcom ein Auftragsverarbeiter ist (d. h. wenn HCPs Patientendaten in Verbindung mit einem Clarity-Klinikkonto verarbeiten, das Krankenhaus über ein speziell mit ihm verknüpftes Patientenkonto auf die Patientendaten zugreift und wenn die Daten von einem Patienten über einen Dexcom-Empfänger im Konto des Krankenhauses auf Dexcom Clarity hochgeladen werden, also wenn keine anderen Dexcom-Dienste (wie z. B. die Dexcom-App) vom Patienten genutzt werden oder wurden), liegt es in der Verantwortung des HCP, die geeignete Rechtsgrundlage für die Verarbeitung der Daten des Patienten durch das CGM-System von Dexcom zu festzustellen. Siehe unter Ziff. 1.2.1) oben für Details.

### **4. Ist die Nutzung Ihrer Cloud-Lösung auf Basis eines Auftragsverarbeitungsvertrags (gem. Art. 28 DSGVO) rechtlich unproblematisch möglich?**

Ja, für die oben beschriebenen Szenarien, in denen sich HCPs als Auftragsverarbeiter gemäß der DSGVO qualifizieren, bieten wir diesen HCPs als unseren Kunden einen Standard-Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO an.

### **5. Werden mit dem Produkt verwaltete Patientendaten und/oder hieraus abgeleitete oder anonymisierte Daten von Ihnen oder Dritten ganz oder teilweise auch für eigene Zwecke genutzt, beispielsweise zu statistischen Zwecken, zur Produktverbesserung oder Forschung? Falls ja, bitte angeben, welche Daten von wem in welcher Form und für welche Zwecke verarbeitet werden.**

Dexcom verarbeitet Patientendaten in Szenarien, in denen es der Auftragsverarbeiter ist, nur für eigene Zwecke, wenn dies gemäß DSGVO zulässig ist, d. h. im Wesentlichen nur in Fällen, in denen

diese Daten ordnungsgemäß anonymisiert werden, in Übereinstimmung mit den bewährten Praktiken jedes anderen Cloud-Diensteanbieters. Um einige weitere Details zu nennen, werden Informationen, die wir für eigene Zwecke verwenden, in unserer Datenschutzerklärung als "abgeleitete Informationen" bezeichnet.

**Abgeleitete Informationen sind Informationen, die durch Kombination oder Analyse anderer Kategorien personenbezogener Daten, die von Patienten erhalten wurden, erstellt wurden. Abgeleitete Informationen können personenbezogene Daten darstellen oder auch nicht. Wenn abgeleitete Informationen personenbezogene Daten darstellen, werden wir sie nur in Übereinstimmung mit den geltenden DSGVO-Anforderungen verwenden (z. B. zur Erfüllung unseres Vertrags mit Patienten oder wenn eine Einwilligung dafür vorliegt, siehe Details unten).**

**Wenn abgeleitete Informationen keine personenbezogenen Daten darstellen (z. B. weil wir sie ordnungsgemäß aggregiert/anonymisiert haben), unterliegen diese Daten nicht mehr der DSGVO. Dennoch hält sich Dexcom natürlich an sonstige Erfordernisse, die für diese nicht-personenbezogenen Daten gelten könnten.**

**Kategorien von persönlichen Daten, aus denen Dexcom abgeleitete Informationen erstellen kann:**

- Informationen zum Standort
- Konto-Informationen
- Informationen zur Bestellung
- Gesundheitsdaten und andere Nutzungsinformationen
- Informationen zur Kommunikation
- Informationen von Drittanbietern
- Sonstige eine Person identifizierbare Informationen.

Wir können die oben genannten Kategorien für Zwecke wie die Softwareentwicklung, die Verwaltung von Benutzereinigigungen und -präferenzen, die Verwaltung von Anbietern und die Durchführung der Debitorenverwaltung kombinieren oder analysieren. Darüber hinaus verwenden wir abgeleitete Informationen zur Verwaltung klinischer Daten für Studien in bestimmten Märkten mit Einwilligung, zur Fehlerverfolgung und -berichterstattung, zur Verwaltung des Identitätszugriffs und für Betrugs- und Sicherheitszwecke.

Ein Beispiel hierfür wäre die Weitergabe von Bestellinformationen an einen Auftragsverarbeiter, der die Annahme von Online-Zahlungen verwaltet.

Wir können Bestellinformationen in Form abgeleiteter Informationen, die nicht identifizierbare Informationen sind, aggregieren und anonymisieren und diese Metrik an einen separaten Dienstleister oder ein verbundenes Unternehmen weitergeben, der/das für die Überwachung des Bestands an Sensoren verwendet wird.

## **6. Welche datenschutzrechtlichen Organisationsmaßnahmen muss der Anwender in Bezug auf das Produkt vornehmen, damit das Produkt datenschutzkonform eingesetzt werden kann?**

In Bezug auf die Rechtsgrundlage als organisatorische Maßnahme hängt dies davon ab, ob HCPs die Einwilligung der Patienten einholen wollen oder nicht. Wie bereits erwähnt, sind wir der Ansicht, dass eine Einwilligung in der Regel nicht erforderlich ist, da die Anforderungen, unter denen HCP's Patientendaten verarbeiten dürfen, gemäß Art. 9(2)(h) DSGVO verarbeiten dürfen (siehe oben unter Abschnitt 1.2.1)).

Abgesehen davon erfordert das Dexcom CGM-System keine Besonderheiten, die über das

hinausgeht, was ohnehin von HCP's in Bezug auf die rechtmäßige Verarbeitung personenbezogener Daten gemäß DSGVO gefordert wird, um die Rechenschaftspflichten der DSGVO zu erfüllen. Dazu gehören u. a. interne Richtlinien und Verfahren zur Zugriffsverwaltung (so dass der Zugriff nur auf einer *Need-to-know*-Basis gewährt wird), Vertraulichkeitsverpflichtungen der Mitarbeiter von HCP's, ein Verarbeitungsverzeichnis, ein Aufbewahrungskonzept usw. HCPs, die die DSGVO ernst nehmen, sollten all diese Aspekte bereits umgesetzt haben.

In Bezug auf die Zugriffsverwaltung als einen wichtigen Teil davon möchten wir betonen, dass der Zugriff auf einen Clarity-Klinik-Account zur Anwendungsnutzung vom Arbeitsplatz des HCP-Benutzers aus gesteuert wird. Mitarbeiterkonten können vom Administrator des HCP-Kontos als Standard- oder Verwaltungsebene bereitgestellt werden. Benutzer der administrativen Ebene können weitere Mitarbeiter zum Zugriff auf das Konto einladen. Jedes Mitarbeiterkonto hat einen individuellen Benutzernamen und ein Passwort. Die Schulung bezüglich der Sicherheit und des Datenschutzes der Konten liegt in der Verantwortung des HCPs. Clarity ermöglicht es administrativen Anwendern, die Sicherheitseinstellungen für Konten anzupassen, einschließlich des Passworts und des Ablaufs bei Inaktivität des Kontos. Dennoch ist dies nur die technische Ebene und HCPs sollten natürlich über Richtlinien verfügen, die in erster Linie die Anforderungen festlegen, wer in welchem Umfang Zugriff erhalten soll.

**7. Wie ist garantiert, dass die mit dem Produkt verwalteten Daten für die Dauer der jeweils geltenden gesetzlich vorgeschriebenen Aufbewahrungsfristen zugänglich sind?**

Wenn Dexcom der Auftragsverarbeiter von Patientendaten für HCPs ist, müssen die geltenden Aufbewahrungsfristen von dem HCP festgelegt werden, der das Dexcom CGM-System einsetzt. Gesundheitsdienstleister können Dexcom jederzeit auffordern, einen Datensatz oder eine Reihe von Datensätzen zu löschen, um ihre Aufbewahrungspflichten zu erfüllen.

Dexcom als multinationaler Dienstleister kann natürlich nicht die Aufbewahrungsfristen für sämtlicher seiner HCP-Kunden festlegen und ist zudem als Auftragsverarbeiter auch nicht gesetzlich dazu verpflichtet.

**8. Ist für die Nutzung des Produkts die dauerhafte Einwilligung des Anwenders und/oder des jeweiligen Patienten in Nutzungsbestimmungen erforderlich? Falls ja: bitte senden Sie uns die aktuelle Fassung der Nutzungsbedingungen**

Siehe oben unter Ziff. 1.2.1). Unserer Ansicht nach ist typischerweise keine Einwilligung erforderlich, wenn ein HCP der Verantwortliche und Dexcom der Auftragsverarbeiter ist.

**9. Welche Kosten fallen für die Nutzung des Produktes an?**

Bitte finden Sie die Preisliste (Listenpreise) vom 10. August 2018 anliegend als Annex 1.

Diabetes-Kliniken erhalten von uns ein individuelles Angebot. Sie können es über unsere Website anfordern: <https://seu2.cleverreach.com/f/157073-207190/>.

**10. Ist die komplette Nutzung des Produkts ohne Installation, d.h. allein per Internet-Browser möglich oder müssen zusätzlich Komponenten wie Treiber, Uploadprogramme oder Dienste lokal installiert werden? Falls eine Installation erforderlich ist: was genau muss installiert werden und welche administrativen Rechte sind dazu erforderlich? Können sich hierdurch Risiken in Bezug auf die IT- Sicherheit der Klinik ergeben?**

Siehe unter Frage 1 - nur in Bezug auf die lokale Konfiguration von HCPs, die retrospektive Überprüfungen und Berichte benötigen. In diesen Fällen kann Dexcom Clarity mit dem dedizierten Empfänger verwendet werden, was eine Installation des Clarity Uploader-Tools auf mindestens einem Krankenhaus-Desktop/Laptop erfordert. Der Clarity Uploader muss auf dem lokalen Rechner installiert werden. Die Client-Software kann von der Clarity-Website heruntergeladen werden. Das Netzwerk muss möglicherweise so konfiguriert werden, dass der Uploader mit der Clarity-Website und dem Server kommunizieren kann. Weitere Details zum Uploader und den Einstellungen finden Sie im Dexcom Clarity Benutzerhandbuch für Kliniken (das wir Ihnen gerne auf Wunsch zukommen lassen). Der dedizierte Empfänger muss dann über USB mit dem Desktop/Laptop verbunden werden, damit die Glukosdaten des Patienten manuell in die Clarity-Webanwendung hochgeladen werden können.

Durch die Installation des Clarity Uploaders ergeben sich jedoch keine Risiken in Bezug auf die IT-Sicherheit der Klinik.

Abgesehen davon, nein. Für den Zugriff auf Clarity ist keine Installation erforderlich, da medizinisches Fachpersonal über einen üblichen Internet-Browser auf Clarity zugreifen kann.

Abschließend möchten wir betonen, dass wir den Schutz personenbezogener Daten und die IT-Sicherheit unserer Produkte und Dienstleistungen sehr ernst nehmen und ständig und proaktiv an deren Verbesserung arbeiten. Personenbezogene Daten unserer Kunden/Patienten und andere von Dexcom verarbeitete personenbezogene Daten werden weltweit in Übereinstimmung mit den geltenden Datenschutzgesetzen, einschließlich der DSGVO, geschützt. Im Einzelnen haben wir die folgenden Maßnahmen ergriffen:

- Um die Einhaltung der Grundsätze der Vertraulichkeit und Integrität zu gewährleisten, haben wir die in unseren Richtlinien beschriebenen technischen und organisatorischen Maßnahmen umgesetzt. In diesem Zusammenhang haben wir z. B. Verschlüsselungsmechanismen sowohl im Ruhezustand als auch während der Übertragung eingerichtet und unterstützen die Verwendung international anerkannter Verschlüsselungsstandards und -algorithmen.
- Darüber hinaus pflegen wir das Sicherheitsmanagement und haben Verfahren implementiert, die sicherstellen, dass unsere Mitarbeiter regelmäßig geschult werden, um die ihnen zugewiesenen Aufgaben in Übereinstimmung mit den Anforderungen des Datenschutzes angemessen zu erfüllen.
- ISO/IEC 27001 beschreibt die Anforderungen für ein Informationssicherheitsmanagementsystem (ISMS), spezifiziert eine Reihe von Best Practices und spezifiziert die Sicherheitskontrollen, die helfen können, Informationsrisiken zu managen. Das Informationssicherheitsmanagementsystem (ISMS) von Dexcom ist von SRI Quality System Registrar (<https://www.sriregistrar.com/>) als konform mit ISO/IEC 27001:2013 zertifiziert.
- Darüber hinaus verwalten wir den Zugriff auf Daten, Anwendungen und Systeminfrastruktur gemäß unseren Unternehmensrichtlinien, um sicherzustellen, dass nur autorisierte Benutzer Zugriff auf diese Daten haben.

Im Zusammenhang mit der IT-Sicherheit ist zu betonen, dass es stets das Ziel von Dexcom ist, möglichen Risiken vorzubeugen und diese zu reduzieren, die Patientensicherheit zu gewährleisten und seine Produkte kontinuierlich zu verbessern. Um die IT-Sicherheit weiter zu verbessern, stellt Dexcom regelmäßig Updates zur Verfügung, führt Penetrationstests durch, implementiert verbesserte IT-Sicherheitslösungen und arbeitet fortlaufend an Produkten der nächsten Generation.

\*\*\*

## BVKD-Geschäftsstelle

---

**Von:** Privacy, Germany <germany.privacy@roche.com>  
**Gesendet:** Dienstag, 11. Mai 2021 15:33  
**An:** BVKD-Geschäftsstelle  
**Betreff:** Re: Fragen zu datenschutzrechtlichen Bedingungen

**Kennzeichnung:** Zur Nachverfolgung  
**Kennzeichnungsstatus:** Erledigt

Sehr geehrter Herr Jannaschk,

vielen Dank für Ihre Nachricht und die erneute Nachfrage. Bitte entschuldigen Sie die verzögerte Rückmeldung.

Die Roche Diabetes Care Deutschland GmbH ist Teil der Roche-Gruppe, die in ihrer Diabetes-Care-Sparte weltweit verschiedene digitale Lösungen anbietet (z. B. die Roche Diabetes Care Plattform und die mySugr-App). Eine pauschale Beantwortung der Fragen für sämtliche Lösungen ist daher nicht ohne Weiteres möglich. Bei den nachfolgenden Antworten konzentrieren wir uns daher auf die "Roche Diabetes Care Plattform", die künftig als zentrale Plattform für Diabetes-Management für den deutschen Markt angeboten werden wird. Da sie sich bislang für den deutschen Markt in der Pilotphase befindet, sind noch einige Änderungen möglich und einige Details noch nicht abschließend geklärt.

Der Dringlichkeit geschuldet, finden Sie bitte nachfolgend die Antworten auf Ihre einzelnen Fragen direkt in dieser E-Mail. Melden Sie sich gerne bei Rückfragen, die wir dann ggf. zusammen mit dem jeweiligen Produkt-Team beantworten können.

Viele Grüße

Florian Schneider

### **Zu Frage 1:**

Die Roche Diabetes Care Plattform ist eine Lösung, bei der Roche als sog. Auftragsverarbeiter für Patientendaten auf Basis einer Auftragsverarbeitungsvereinbarung mit den Kliniken als datenschutzrechtlich Verantwortliche tätig wird. Das Vorhandensein Rechtsgrundlage für die Verarbeitung der Patientendaten ist dementsprechend durch die Kliniken sicherzustellen. In der Regel wird die Datenverarbeitung auf eine Einwilligung der Patient:innen gestützt.

### **Zu Frage 2:**

Die Server, auf denen die Daten gespeichert sind und verarbeitet werden, befinden sich in einem Datenzentrum in Frankfurt am Main, das von Amazon Web Services, Inc ("AWS") betrieben wird. Das Management der Plattform (Infrastruktur, Operations, Sicherheit) erfolgt durch den Dienstleister Accenture aus der Schweiz (für die ein sog. Angemessenheitsbeschluss der EU-Kommission besteht) und Spanien heraus. Mit dem Anbieter AWS sind sog. EU-Standardvertragsklauseln vereinbart, die zusammen mit weiteren Maßnahmen eine datenschutzkonforme Verarbeitung sicherstellen sollen.

### **Zu Frage 3:**

Unsere Kunden (z. B. Kliniken) sind die datenschutzrechtlich Verantwortlichen, Roche ist Auftragsverarbeiter. Wir fordern unsere Kunden daher auf, eine Rechtsgrundlage für die Datenverarbeitung sicherzustellen. Dies ist typischerweise die Einwilligung der Patient:innen. Die Roche Diabetes Care Plattform unterstützt dieses Vorgehen, indem die Healthcare Professionals (HCP) beim ersten Login ein Fenster angezeigt bekommen, wo bestätigt werden muss, dass nur Patient:innen hinzugefügt werden, die in die Nutzung eingewilligt haben (sofern dies im jeweiligen Land gesetzlich vorgesehen ist).

**Zu Frage 4:**

Roche stellt eine Auftragsverarbeitungsvereinbarung gemäß Artikel 28 Datenschutz-Grundverordnung zur Verfügung. Das jeweils anwendbare Recht hängt allerdings von dem jeweiligen Kunden als datenschutzrechtlich Verantwortlichen ab. Im Zusammenhang mit (insbesondere staatlichen) Zugriffsmöglichkeiten auf Daten aus sog. Drittstaaten gibt es vor dem Hintergrund des Schrems II-Urteils des Europäischen Gerichtshofs vom 16. Juli 2020 (Rechtssache C-311/18) aktuell eine breite und intensiv geführte Debatte, welche Voraussetzungen bei der Einbindung von Unternehmen mit (Haupt-)Sitz in diesen Drittstaaten konkret zu gewährleisten sind.

**Zu Frage 5:**

Roche behält sich derzeit vor, anonymisierte Daten für Service- und Produktverbesserungen zu nutzen. Dies wird in der zukünftigen Datenschutzerklärung und den Nutzungsbedingungen näher beschrieben werden.

**Zu Frage 6:**

Im Zusammenhang mit der Nutzung der Roche Diabetes Care Platform sind in der Regel Einwilligungen der Patient:innen einzuholen, was etwa im Rahmen der bestehenden Prozesse innerhalb einer Klinik geschehen kann. Daneben sind die üblichen Maßnahmen im Rahmen des Einsatzes von IT-Lösungen in Kliniken zu treffen, etwa dass personengebundene Zugänge nicht von mehreren Personen gemeinsam genutzt werden oder unberechtigte Dritte Einblick in Bildschirminhalte erhalten.

**Zu Frage 7:**

Die Roche Diabetes Care Platform darf nicht als Ersatz für die (elektronische) Patientenakte verwendet werden. Entsprechend sollten behandlungs- bzw. beratungsrelevante Patienteninformationen heruntergeladen oder ausgedruckt werden.

**Zu Frage 8:**

Ja, die Zustimmung zu den Nutzungsbedingungen muss von einem Vertreter der Klinik erteilt werden. In der aktuellen Ausgestaltung müssen Patient:innen nicht in Nutzungsbedingungen der Roche Diabetes Care Platform einwilligen.

**Zu Frage 9:**

Die Nutzung der Roche Diabetes Care Platform setzt für sog. Premium-Module einen kostenpflichtigen Vertrag voraus. Da es bis zur Markteinführung in Deutschland allerdings noch Änderungen geben kann, können wir zum aktuellen Zeitpunkt keine Details nennen.

**Zu Frage 10:**

Technisch kann die Roche Diabetes Care Platform vollständig und ohne Einschränkungen mittels eines Internet-Browsers verwendet werden (sog. Software-as-a-service). Es besteht zudem die Möglichkeit, auf den Klinik-PC eine Upload-Funktion (Treiber) zu installieren, mit der Daten von Blutzuckermessgeräten direkt auf die Plattform hochgeladen werden können. Diese setzt nur für die Installation Administratorrechte voraus.

**Dr. Florian Schneider**

Konzerndatenschutzbeauftragter Deutschland | Group Data Protection Officer Germany

Syndikusrechtsanwalt | Legal Counsel

Roche Deutschland Holding GmbH

Emil-Barell-Straße 1  
D-79639 Grenzach-Wyhlen  
Büro.: +49 (0)7624 14-2983  
Mobil: +49 (0)172 639-3612  
Fax: +49 (0)7624 14-3819  
E-Mail: [florian.schneider.fs3@roche.com](mailto:florian.schneider.fs3@roche.com)  
[www.roche.de](http://www.roche.de)

**Roche Deutschland Holding GmbH** | Sitz der Gesellschaft: Grenzach-Wyhlen | Registergericht: Freiburg, HRB 412761 | Geschäftsführung: Dr. Marc Bächli, Vorsitzender; Christian Paetzke, Prof. Dr. Hagen Pfundner, Claus Haberda, Andreas Schmitz, Ulrich Winkel | Aufsichtsratsvorsitzender: Dr. Thomas Schinecker

### Privacy Office Germany

Roche Diagnostics GmbH  
LDB.....6164  
Sandhofer Strasse 116  
68305 Mannheim / Germany  
<mailto:germany.privacy@roche.com>

### Roche Diagnostics GmbH

Sandhofer Straße 116; D-68305 Mannheim; Telefon +49-621-759-0; Telefax +49-621-759-2890  
Sitz der Gesellschaft: Mannheim - Registergericht: AG Mannheim HRB 3962 - Geschäftsführung: Claus Haberda; Andreas Schmitz -  
Aufsichtsratsvorsitzender: Dr. Thomas Schinecker

### Confidentiality Note

This message is intended only for the use of the named recipient(s) and may contain confidential and/or privileged information. If you are not the intended recipient, please contact the sender and delete the message. Any unauthorized use of the information contained in this message is prohibited.

Am Fr., 7. Mai 2021 um 12:12 Uhr schrieb BVKD-Geschäftsstelle <[geschaeftsstelle@die-diabetes-kliniken.de](mailto:geschaeftsstelle@die-diabetes-kliniken.de)>:

Sehr geehrte Damen und Herren,

am 05.03.2021 haben wir Ihnen per Brief (siehe Anlage) einige Fragen zu datenschutzrechtlichen Bedingungen zukommen lassen, die bei der Nutzung von Daten, die von Blutzuckermessgeräten bzw. –sensoren und Insulinpumpen erhoben und im Krankenhaus verarbeitet werden. Darauf haben wir von Ihnen bisher keine Antwort erhalten.

Da wir am 12. Mai 2021 im Rahmen des Symposiums "IT, Datenschutz und Datensicherheit im Krankenhaus" im Rahmen des Diabetes Kongresses der Deutschen Diabetes Gesellschaft über diese Fragen berichten wollen, würden wir uns sehr freuen, wenn Sie uns kurzfristig noch eine Antwort auf unser Schreiben zukommen lassen könnten.

Freundliche Grüße

Klaus-Dieter Jannaschk  
Bundesverband Klinischer Diabetes-Einrichtungen  
DIE Diabetes-Kliniken e.V.  
Bundes-Geschäftsstelle



Kirchberg 21  
37431 Bad Lauterberg

Tel: 05524/ 81218

Fax: 05524/ 81398

E-Mail: [geschaefsstelle@bvkd.de](mailto:geschaefsstelle@bvkd.de)

Internet: [www.bvkd.de](http://www.bvkd.de)



**[Hier geht es zu unserer neuen Image-Broschüre ...](#)**

An den  
Bundesverband Klinischer Diabetes-Einrichtungen  
DIE Diabetes-Kliniken e. V.  
Bundes-Geschäftsstelle  
Kirchberg 21  
37431 Bad Lauterberg

Berlin, am 25. März 2021

Antwort auf Ihr Schreiben „Fragen zu datenschutzrechtlichen Bedingungen“  
vom 5. März 2021

Sehr geehrter Herr Jannaschk,

gerne senden wir Ihnen Informationen zu der Cloud-Lösung, die wir als A. MENARINI DIAGNOSTICS Deutschland - eine Division der BERLIN-CHEMIE AG (folgend „das Unternehmen“) derzeit vertreiben. Das Unternehmen vertreibt aktuell die folgenden Produkte, bei denen ein Datenaustausch per Cloud-Verbindung optional und nach Freigabe durch den Anwender möglich ist:

- **Glucomen Day<sup>®</sup> CGM**: Ein rtCGM-System zur kontinuierlichen Glukosemessung, wobei per Bluetooth die gemessenen Glukosewerte in die Glucomen Day<sup>®</sup> App übertragen werden.
- **Glucolog<sup>®</sup> web Software**: Glucomen Day<sup>®</sup> CGM Daten aus der Glucomen Day<sup>®</sup> App können vom Nutzer optional in eine Cloud hochgeladen werden und über die Cloud Software Glucolog<sup>®</sup> web analysiert werden.

Unsere klassischen Blutzuckermessgeräte, nach denen Sie ja auch gefragt haben, nutzen keine Cloud-Lösung und speichern Messwerte ausschließlich im Gerät selbst.

Folgend senden wir Ihnen gerne genauere Informationen zu den beiden o.a. Produkten mit optionaler Cloud-Anbindung:



## GlucoMen Day® CGM

GlucoMen Day® CGM ist ein System zur kontinuierlichen Glukosemessung. Die Glukosewerte werden in die dazugehörige GlucoMen Day® App über Bluetooth übertragen. Nutzer können optional die Daten aus der App in die Cloud des Herstellers WaveForm Technologies Inc./AgaMatrix Inc. senden. Die Daten können aus der Cloud, nur nach Zustimmung des Nutzers, in andere Softwarelösungen hochgeladen werden. Eine dieser Softwarelösungen zum Weiterverarbeiten wird über A. MENARINI Diagnostics vertrieben: GlucoLog® web Software. Nähere Informationen finden Sie untenstehend. Der Hersteller von GlucoMen Day® CGM, der auch datenschutztechnisch verantwortlich für das Produkt (inkl. Cloud-Lösung) ist, ist WaveForm Technologies Inc./AgaMatrix Inc.. Die Daten werden dabei in der Europäischen Union (EU) auf durch AgaMatrix kontrollierten Servern gespeichert, auf denen die Verarbeitung der Daten in Übereinstimmung mit dem EU-Recht erfolgt. A. MENARINI DIAGNOSTICS, eine Division der BERLIN-CHEMIE AG ist ausschließlich Vertriebspartner. GlucoMen Day® CGM ist ein Medizinprodukt der Klasse IIb. Es ist zertifiziert nach der Medizinprodukte-Richtlinie 93/42/EWG und trägt das Kennzeichen CE1304. Das aktuelle Zertifikat der Benannten Stelle ist gültig bis 27.05.2024. Es schließt das gesamte GlucoMen Day® CGM System, sowie die GlucoMen Day® App ein. Die App ist somit als ein Medizinprodukt zertifiziert.

## GlucoLog® web Software

Die Cloud-Software kann über die Website [www.glucoLogweb.com](http://www.glucoLogweb.com) geöffnet werden. Die Nutzung des Produkts ist ohne Installation, d.h. allein per Internet Browser, möglich. Der Hersteller der Software ist Zucchetti Centro Sistemi S.p.A in Italien. A. MENARINI Diagnostics ist ebenfalls Vertriebspartner. Der Hersteller ist datenschutzrechtlich für das Produkt verantwortlich. Die Software ist nicht zertifiziert, da sie nicht unmittelbar zum Treffen von Behandlungsentscheidungen vorgesehen ist. Die Nutzung ist für Patienten kostenlos. Medizinisches Fachpersonal kann die Software für einmalig 49 Euro über den Webshop auf der Website [www.glucomenday.de](http://www.glucomenday.de) erwerben.

Im Fall von Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.  
Mit freundlichen Grüßen.

i.V. Dr. Julia Wernicke  
Datenschutzbeauftragte

i.V. Albert Sauter  
Verkaufsleiter

Bundesverband Klinischer Diabetes-Einrichtungen  
Bundes-Geschäftsstelle  
Klaus-Dieter Jannaschk  
Kirchberg 21  
37431 Bad Lauterberg

Ypsomed AG  
Brunnmattstrasse 6  
Postfach  
3401 Burgdorf / Schweiz  
Tel. +41 34 424 41 11  
Fax +41 34 424 41 22  
www.ypsomed.com  
info@ypsomed.com

Burgdorf, 25. Mai 2021

## **Antworten zu datenschutzrechtlichen Bedingungen**

Sehr geehrter Herr Jannaschk

Gerne beantworten wir Ihre Fragen aus dem Schreiben vom 5. März 2021 bezüglich der datenschutzrechtlichen Bedingungen bei der Nutzung unserer mylife Software und entschuldigen uns für die lange Bearbeitungszeit.

Als international tätiges Unternehmen für Herstellung und Vertrieb von Medizinprodukten haben wir den Anspruch, die geltenden Gesetze in unserem Tätigkeitsgebiet einzuhalten. Insbesondere der Schutz personenbezogener Daten ist der Ypsomed aufgrund der hohen Sensibilität von Gesundheitsdaten ein grosses Anliegen.

1. *Auf welcher Rechtsgrundlage erfolgen die zur Nutzung der von uns angebotenen mylife Cloud-Lösungen (im Folgenden „Produkt“) erforderlichen Datenbearbeitungsvorgänge?*

Die mylife Software ist ein Online-Diabetes-Tagebuch, mit dem registrierte Anwender ihre Daten speichern und auswerten können. Die Nutzung des Produkts unterliegt den Allgemeinen Geschäftsbedingungen und den Datenschutzrichtlinien, die der Anwender bei der Registrierung für das Produkt akzeptiert.

Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten in der mylife Software stützen wir primär auf die Erfüllung unserer vertraglichen Verpflichtungen gegenüber den registrierten Anwendern gemäss Art. 6 Abs. 1b DSGVO.

Für die Verarbeitung personenbezogener Daten der besonderen Kategorie (Therapiedaten) erteilt der Anwender seine Einwilligung mit der Registrierung für eine Patientenkonten. Unsere Rechtsgrundlage stützen wir hier auf Art. 9 Abs. 2a DSGVO.

Weiter kann der Anwender seine eigenen Daten mit anderen Anwendern des Systems (z.B. Ärzte, Kliniken) teilen und diese Teilung jederzeit widerrufen. In diesem Fall beruht die Verarbeitung auf der Einwilligung des Anwenders nach Art. 6 Abs. 1a DSGVO sowie Art. 9 Abs. 2a DSGVO.

2. *Erfolgt die Datenverarbeitung ausschliesslich innerhalb der EU?*

Für den Schutz der personenbezogenen Daten nutzen wir bezüglich der von der mylife Software erhobenen Therapie- und Geräte-Daten die Cloud-Dienste von Microsoft (Windows Azure). Die Daten werden in Europa gespeichert.

Die Verarbeitung der personenbezogenen Daten erfolgt durch die SINOVO health solutions GmbH (SINOVO), die im CE Markt Inverkehrbringerin der mylife Software ist. Ypsomed AG hat keinen Zugriff auf die Daten in der App und der Cloud.

3. *Ist für die mit der Nutzung des Produkts verbundenen Datenübermittlungs- und Verarbeitungsvorgänge eine Einwilligung der Patienten erforderlich?*

Die Patienten entscheiden freiwillig, mit wem sie ihre Daten teilen wollen (z.B. Ärzte, Kliniken). Bevor die Ärzte resp. die Klinik aus ihrem eigenen Klinikkonto eine Einladung an den jeweiligen Patienten übermitteln, seine Online-Daten mit der Klinik zu teilen, müssen sie vom Patienten eine Einverständniserklärung unterzeichnen lassen. Gegenüber der mylife Software bestätigen sie, dass diese Einverständniserklärung eingeholt wurde.

Sobald der Patient die Datenfreigabe in seinem Patientenkonto aktiviert und in die Datenübermittlung einwilligt, kann die Klinik direkt auf die Daten des Patienten zugreifen, Daten hinzufügen, bearbeiten oder neu anlegen. Die Daten der Klinik und die Daten des Patienten werden zusammengeführt.

Der Patient kann die Datenfreigabe jederzeit widerrufen resp. beenden. Die Klinik hat ab diesem Zeitpunkt keinen Zugriff mehr auf die Daten dieses Patienten. Im Klinikkonto scheint es, als ob dieser Patient gelöscht ist. Die Klinik wird durch eine E-Mail vom mylife Server informiert, wenn der Patient die Datenfreigabe beendet.

4. *Ist die Nutzung Ihrer Cloud-Lösung auf Basis eines Auftragsverarbeitungsvertrags (gem. Art. 28 DSGVO) rechtlich unproblematisch möglich?*

Die Nutzung unserer mylife Cloud basiert nicht auf einer Auftragsverarbeitung gem. Art.28 DSGVO. Die mylife Cloud wird im Auftrag der Ypsomed durch die SINOVO entwickelt und gewartet. SINOVO verarbeitet die Daten gemäss den Grundsätzen aus Art.5 DSGVO.

Mit der Registrierung auf ein Konto in der mylife Cloud werden die Anwender transparent und in verständlicher Weise über die Verarbeitung der Daten informiert und auf ihre Rechte hingewiesen. Mit bestätigen und akzeptieren dieser Informationen entsteht zwischen dem Kontoinhaber und der SINOVO ein Dienstleistungsvertrag.

Die Datenfreigabe zwischen den Kontoinhabern (Patient und Klinik) erfolgt aufgrund deren gemeinsamen und übereinstimmenden Willensäusserung (Einwilligung). Jeder Kontoinhaber hat das Recht, seine Kontodaten selbständig zu verwalten und Änderungen vorzunehmen. SINOVO stellt dazu die geeigneten Mittel zur Verfügung und wahrt die Rechte der einzelnen Anwender. Weder SINOVO noch Ypsomed nehmen im Auftrag oder selbständig Änderungen an den Einträgen und Daten vor, es sei denn, SINOVO ist gesetzlich dazu verpflichtet.

5. *Werden mit dem Produkt verwaltete Patientendaten und/oder hieraus abgeleitete oder anonymisierte Daten durch Ypsomed oder Dritte ganz oder teilweise auch für eigene Zwecke genutzt, beispielsweise zu statistischen Zwecken, zur Produktverbesserung oder Forschung? Falls ja, bitte angeben, welche Daten von wem in welcher Form und für welche Zwecke verarbeitet werden.*

Die mylife Software wird im Auftrag der Ypsomed durch die SINOVO betrieben. Ypsomed hat keinen Zugriff auf die Daten in der mylife Software. SINOVO verwendet anonymisierte und aggregierte Daten für die geforderte Marktüberwachung nach MDD / MDR sowie für statistische Auswertungen. Ypsomed erhält auf Antrag lediglich anonyme Daten für statistische Zwecke. Gesundheitsdaten verarbeitet SINOVO zu keinen anderen Zwecken als der Erbringung der Dienstleistungen über die mylife Software.

Die statistischen Auswertungen dienen

- der Bereitstellung, Aufrechterhaltung, Verbesserung und Entwicklung von relevanten Funktionen, Inhalten und Diensten unserer Produkte.
- der Aufdeckung und Abwehr von betrügerischen, missbräuchlichen und verbotenen Aktivitäten sowie dem Schutz und der Sicherheit unserer Dienste.

Die Kontodaten werden in keinem Fall zur Erstellung von Anwenderprofilen - gleich welcher Art - verwendet.

6. *Welche Datenschutzrechtlichen Organisationsmassnahmen muss der Anwender in Bezug auf das Produkt vornehmen, damit das Produkt datenschutzkonform eingesetzt werden kann.*

Der Anwender muss die Nutzungsbedingungen für das Produkt beachten und ist insbesondere für die Geheimhaltung seiner Zugangsdaten inklusive Passwort verantwortlich. Eine Weitergabe sowie das Zugänglichmachen der Zugangsdaten sowie des Passwortes an bzw. gegenüber Dritten sind unzulässig. Der Anwender übernimmt die Verantwortung für sämtliche Handlungen, die unter Verwendung seiner Zugangsdaten getätigt werden.

Die Klinik und ihre Anwender beachten bei der Verarbeitung der personenbezogenen Daten in der mylife Cloud die geltenden Datenschutzgesetze.

7. *Wie ist garantiert, dass die mit dem Produkt verwalteten Daten für die Dauer der jeweils geltenden gesetzlich vorgeschriebenen Aufbewahrungsfristen zugänglich sind.*

Das mylife Therapiemanagement dient zur Protokollierung der relevanten Therapiedaten und wurde mit dem Ziel einer optimierten Kommunikation zwischen Menschen mit Diabetes und medizinischem Fachpersonal entwickelt. Die mylife Software dient lediglich als Hilfsmittel zur Protokollierung der eingegebenen Therapiedaten. Die mylife Software kann in keiner Weise die ärztliche Beratung und Therapieplanung oder die Dokumentation im Patientendossier ersetzen.

Die Datensicherungen ausserhalb der mylife Cloud muss regelmässig von der Klinik durchgeführt werden, damit die Daten nicht unbeabsichtigt verloren gehen bzw. damit die Überwachung auf anderem Wege sichergestellt werden kann. Die Daten werden nur so lange in der mylife Cloud aufbewahrt, wie es für den Zweck der Datenprotokollierung oder für den Zeitraum, in dem das Patientenkonto aktiv ist, erforderlich ist. Der registrierte Anwender kann sein Konto jederzeit schliessen. Die gespeicherten Daten werden gelöscht, soweit SINOVO nicht zur Erfüllung gesetzlicher Pflichten oder zur Beilegung von Streitigkeiten zur Aufbewahrung der Daten verpflichtet ist.

Wenn der Anwender sein Konto zwei Jahre lang nicht aktiv nutzt, werden seine personenbezogenen Daten aus dem System gelöscht, es sei denn, wir sind in gutem Glauben, dass wir gesetzlich oder anderweitig verpflichtet sind, sie aufzubewahren (z. B. eine Anfrage im Zusammenhang mit einem wahrscheinlichen Rechtsstreit).

8. *Ist die Nutzung des Produkts, die dauerhafte Einwilligung des Anwenders und/oder des jeweiligen Patienten in Nutzungsbestimmungen erforderlich?*

Ja, siehe AGBs im Anhang.

9. *Welche Kosten fallen für die Nutzung des Produktes an?*

Die Nutzung der mylife Software ist für die Patienten kostenlos. Ärzte und Kliniken können die mylife Software für EURO 297.50 erwerben.

- 10 *Ist die komplette Nutzung des Produkts ohne Installation, d.h. allein per Internet-Browser möglich oder müssen zusätzliche Komponenten installiert werden?*

Ärzte und Kliniken können die mylife Software als CD über unseren Online-Shop bestellen. Die mylife Software ist mit verschiedenen Geräten kompatibel.

Systemanforderungen für die Installation der mylife Software:

- Betriebssystem Windows 7 oder neuer
- .NET Runtime-Umgebung Version 4.5 oder neuer (Treiber wird automatisch installiert)
- Benutzer benötigt Administratorrechte, um die mylife Software zu installieren
- 1 GB RAM
- 500 MB Festplattenspeicherplatz

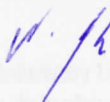
Wir freuen uns, wenn wir Ihre Fragen beantworten konnten und Ihre Mitglieder den Vorteilen unserer mylife Software positiv entgegenstehen.

Freundliche Grüsse  
Ypsomed AG

Stefan Ebener  
Produktmanager



Nadia Glaus  
Datenschutzbeauftragte



- Allgemeine Nutzungs- und Geschäftsbedingungen der SINOVO health solutions GmbH
- Datenschutzrichtlinie der SINOVO health solutions GmbH



## **Allgemeine Nutzungs- und Geschäftsbedingungen der SINOVO health solutions GmbH**

### **A. Allgemeine Bedingungen für die Nutzung unserer Angebote**

#### **1. Allgemeine Hinweise**

a) Wir möchten Sie darauf hinweisen, dass die dargestellten Informationen, Daten und Dienste keine therapeutische Funktion übernehmen können und in keinem Falle einen Arztbesuch ersetzen können. Im Falle gesundheitlicher Probleme sollten Sie unbedingt den Arzt Ihres Vertrauens aufsuchen. Nur der behandelnde Arzt kann eine Diagnose stellen und erforderliche Therapien einleiten.

Bitte beachten Sie die folgenden Bestimmungen für die Nutzung unserer Angebote und unsere separate Datenschutzrichtlinie unter <https://mylife-software.net/privacy>. Mit der Nutzung der auf unseren Seiten angebotenen Informationen, Dienste und Programme erklärt der Nutzer sein Einverständnis mit den hier formulierten Bedingungen.

Die nachfolgenden Bedingungen gelten für die Nutzung der mylife™ Software nebst allen weiteren Online-Angeboten auf dieser Website.

b) Die Internetseiten der SINOVO health solutions GmbH unterliegen regelmäßigen Veränderungen und Ergänzungen, die der Aktualisierung der angebotenen Informationen dienen. Die SINOVO health solutions GmbH übernimmt jedoch keine Haftung oder Garantie für Aktualität, Richtigkeit, Vollständigkeit und Verfügbarkeit der dargestellten Informationen. Der Nutzer kann sich über den Stand der Informationen und Daten unter <http://mylife-software.net> informieren. Die hier dargestellten Informationen und Daten dienen dem Nutzer ausschließlich zu Informationszwecken und zum persönlichen Gebrauch. Die SINOVO health solutions GmbH haftet für direkte oder indirekte Vermögensschäden, einschließlich entgangenen Gewinns, aus der Nutzung des Informationsangebotes dieser Seiten nur bei vorsätzlichem oder grob fahrlässigem Verhalten, sowie in den Fällen zwingender gesetzlicher Vorschriften. Bei direkten oder indirekten Verweisen auf fremde Internetseiten ("Links"), die außerhalb des Verantwortungsbereiches der SINOVO health solutions GmbH liegen, haftet die SINOVO health solutions GmbH nur bei Kenntnis der Inhalte und technischer Möglichkeit und Zumutbarkeit, die Nutzung im Falle rechtswidriger Inhalte zu verhindern.

c) Die SINOVO health solutions GmbH erklärt hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der gelinkten Seiten hat der Anbieter keinerlei Einfluss. Er distanziert



sich ausdrücklich von den Inhalten sämtlicher verlinkter Seiten, die nach der Linksetzung verändert wurden. Diese Feststellung gilt für alle innerhalb des eigenen Internetangebotes gesetzten Links und Verweise. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotener Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde. Der Inhalt dieser Web-Site ist urheberrechtlich geschützt. Die Speicherung des Inhalts ist lediglich zu privaten Zwecken gestattet. Eine kommerzielle Nutzung zur Weiterveröffentlichung oder kostenlosen Verteilung darf nur in Absprache mit der SINOVO health solutions GmbH erfolgen. Sämtliche Hinweise unterliegen der Aktualisierung. Interaktive Angebote dieser Internetseiten können nicht ständig kontrolliert werden. Nutzer sind verpflichtet, auf die Einhaltung der gesetzlichen Bestimmungen zu achten. Die SINOVO health solutions GmbH behält sich ausdrücklich vor, rechtswidrige, anstößige und sachfremde Inhalte zu löschen. Sollten Ihnen dennoch Inhalte auffallen, die Sie als anstößig, rechtswidrig oder sachfremd erachten, bitten wir Sie um entsprechende Mitteilung unter [webmaster@sinovo.net](mailto:webmaster@sinovo.net).

d) SINOVO health solutions GmbH übernimmt keine Gewähr dafür, dass die Inhalte den Erwartungen des Nutzers entsprechen oder er mit den Inhalten ein bestimmtes, von ihm verfolgtes Ziel erreicht. SINOVO health solutions GmbH übernimmt keine Gewähr dafür, dass dem Nutzer das Portal an bestimmten Zeiten zur Verfügung steht. Insbesondere übernehmen wir daher keine Gewähr im Falle von Störungen, Unterbrechungen oder einem etwaigen Ausfall des Portals. Wir weisen darauf hin, dass wir uns die Inhalte der MicroSites sowie der Banner und sonstiger Werbeflächen nicht zu Eigen machen, und keine Gewähr für diese übernehmen.

e) Mit Fragen, Hinweisen oder Anregungen zu diesen Nutzungsbedingungen oder zu dem Internetangebot der SINOVO health solutions GmbH wenden Sie sich bitte per E-Mail an [webmaster@sinovo.net](mailto:webmaster@sinovo.net)

## **2. Datenschutz**

Der Schutz Ihrer personenbezogenen Daten ist für SINOVO health solutions GmbH ein zentrales Anliegen. Die SINOVO health solutions GmbH nimmt den Datenschutz ernst und gestaltet ihr Angebot gemäß den gesetzlichen Bestimmungen für den Datenschutz. Einzelheiten zu unserer Datenschutzrichtlinie können Sie unter <https://mylife-software.net/privacy> entnehmen, die die Allgemeinen Nutzungs- und Geschäftsbedingungen der SINOVO health solutions GmbH ergänzen.

## **3. Geistiges Eigentum**

Alle Copyrights, Handelsmarken und jedes andere geistige Eigentum bezogen auf Materialien oder Inhalte unserer Services gehören ohne Einschränkung der SINOVO health solutions GmbH oder unseren (Lizenz)Partnern. Sie dürfen diese Materialien oder Inhalte nur mit schriftlicher Genehmigung von SINOVO health solutions GmbH oder unseren (Lizenz)Partnern kopieren, reproduzieren, übermitteln, verteilen, verändern oder kommerziell nutzbar machen.

Durch Übermittlung von Materialien an unsere Services fällt uns oder unseren (Lizenz)Partnern das dauerhaft von Gebühren befreite nicht exklusive Nutzungsrecht innerhalb unserer Services und

anderweitiger Art zu. Das Nutzungsrecht beinhaltet auch das Kopieren, Verteilen, Senden, Übermitteln, Anpassen und Editieren des Materials.

#### **4. Widerrechtliche Nutzung der Inhalte**

Die Nutzung der in dem Angebot der SINOVO health solutions GmbH enthaltenen Daten zu Marketingzwecken ist untersagt. Dies umfasst die automatische so wie die manuelle Auslesung der enthaltenen Daten, insbesondere Daten der SINOVO health solutions GmbH sowie etwaige veröffentlichte Daten Dritter, sowie Links zu deren Internetangeboten und E-Mailadressen, Namen und sonstige Daten. Zuwiderhandlungen werden im Rahmen der gesetzlichen Bestimmungen verfolgt.

## **B. Zugang und Nutzung der Leistungen der mylife™ Software Online-Version und Nutzung der mylife™ App der SINOVO health solutions GmbH**

### **1. Allgemeines**

a) Für die Nutzung der Dienste von mylife™ Software Online-Version oder der mylife™ App der SINOVO health solutions GmbH ist eine Internetverbindung notwendig. Für die Verwendung der notwendigen Hardware ist alleine der Nutzer verantwortlich. Entstehende Verbindungskosten oder Übertragungskosten sind vom Nutzer zu tragen. Für die Nutzung der mylife™ App ist zudem ein mobiles Endgerät erforderlich, welches gewisse Systemanforderungen erfüllt. Die SINOVO health solutions GmbH ist nicht für die Einhaltung der Systemanforderungen verantwortlich. Dies obliegt ausschließlich dem Nutzer.

Der Nutzer ist für die Richtigkeit der Login-Informationen und Informationen, die im Rahmen der Registrierung an SINOVO health solutions GmbH übermittelt werden, allein verantwortlich.

Ebenso ist der Nutzer für die Geheimhaltung seiner Zugangsdaten inklusive Passwort selber verantwortlich. Eine Weitergabe sowie das Zugänglichmachen der Zugangsdaten sowie des Passwortes an bzw. gegenüber Dritten sind unzulässig. Sofern der Zugang zu der mylife™ App einer Registrierung des Nutzers bedarf, ist der Nutzer dafür verantwortlich, dass sein Passwort keinem Dritten zugänglich ist. Der Nutzer übernimmt die Verantwortung für sämtliche Handlungen, die unter Verwendung seiner Zugangsdaten getätigt werden.

Der Nutzer wird außerdem angehalten, bei unerlaubtem Gebrauch von Login und Passwort oder bei Unregelmäßigkeiten, welche die Sicherheit betreffen, umgehend SINOVO health solutions GmbH zu informieren.

Durch die Dienste der mylife™ Software Online-Version und der SINOVO health solutions GmbH dürfen keine belästigenden, verleumderischen, rassistischen, diskriminierenden, Gewaltverherrlichenden, obszönen, pornographischen oder bedrohende Inhalte oder sonstigen rechtswidrigen Inhalte übermittelt werden.

Darüber hinaus darf die mylife™ Software und alle Dienste der SINOVO health solutions GmbH nicht in einer Art benutzt werden, welche zum Abbruch, Schaden oder verminderter Leistung führen kann und die Rechte Dritter verletzt. Dazu zählen auch das Recht auf geistiges Eigentum, das Recht auf Vertraulichkeit sowie datenschutzrechtliche Bestimmungen.

Beratungsangebote wie etwa die Hotline der SINOVO health solutions GmbH oder die zentrale Rufnummer sind Angebote, die erreichbar sind mittels der aufgeführten Kontaktdaten. Das Beratungsangebot kann keine individuellen Diagnosen, Behandlungen oder Therapieempfehlungen ersetzen, sondern nur allgemeine und abstrakte, vom Patienten unabhängige, Gesundheitsinformationen liefern. Die Nutzer des Beratungsangebotes sind unbedingt gehalten, sich hinsichtlich ihrer individuellen Diagnose und Behandlung an den Arzt ihres Vertrauens zu wenden und alle Maßnahmen, die im Zusammenhang mit ihrer Gesundheit stehen, mit diesem abzusprechen.

SINOVO health solutions GmbH behält sich das Recht vor, Informationen über die Anrufe zu speichern in Form von Gesprächsnotizen. Anrufe mit betrügerischer Natur, böser Absicht oder Schwindel können strafrechtliche Konsequenzen nach sich ziehen.

b) Die SINOVO health solutions GmbH erbringt alle Leistungen im Zusammenhang mit dem Dienst mylife™ Software Online-Version oder der mylife™ App gegenüber Nutzern, Ärzten, Patienten oder Vertrauenspersonen (im Folgenden: "Kunde") ausschließlich auf Grundlage dieser Allgemeinen Nutzungs- und Geschäftsbedingungen (AGB). Andere AGB finden nur Anwendung, soweit dies von der SINOVO health solutions GmbH einzelvertraglich bestätigt wurde. Die SINOVO health solutions GmbH ist berechtigt, diese AGB mit einer angemessenen Ankündigungsfrist zu ändern oder zu ergänzen. Die Ankündigung erfolgt per E-Mail durch Übersendung der geänderten AGB oder durch E-Mail mit dem Hinweis auf die Möglichkeit der Einsicht der geänderten AGB im Internet auf den Seiten der SINOVO health solutions GmbH unter <https://mylife-software.net/terms>. Widerspricht der Kunde den geänderten oder ergänzten Bedingungen nicht innerhalb von sechs Wochen nach deren Veröffentlichung im Internet, so werden die geänderten oder ergänzenden Bedingungen wirksam. Widerspricht der Kunde fristgemäß, so sind beide Vertragspartner berechtigt, den Vertrag zu dem Zeitpunkt zu kündigen, an dem die geänderten oder ergänzenden Geschäftsbedingungen in Kraft treten sollen.

## **2. Art und Ausführung der Leistungen durch die SINOVO health solutions GmbH**

a) Die Leistung der SINOVO health solutions GmbH umfasst die Bereitstellung der mylife™ Software Online-Version, die Bereitstellung der mylife™ App, eines Online-Daten-Management Systems und Diabetes-Tagebuches für die Kunden, mittels dessen die Diabeteswerte (z.B. Blutzuckermesswerte, Blutdruckmesswerte oder Insulinpumpenmesswerte) der Patienten von jedem beliebigen Ort aus eingetragen, verwaltet und eingesehen werden können.

b) Die SINOVO health solutions GmbH übernimmt mit der Bereitstellung der mylife™ Software oder der mylife™ App keinerlei ärztliche Tätigkeiten, gibt keine therapeutischen Hinweise und erbringt keine Leistungen, die Tätigkeiten eines Arztes ersetzen können oder sollen.

c) Die Freischaltung des Zugangs zur mylife™ Software Online-Version erfolgt nach Vertragsabschluss mit dem Kunden.

d) Soweit die SINOVO health solutions GmbH über die in Ziffer 2 a) genannten vertraglichen Leistungen hinaus freiwillige unentgeltliche Dienste und Leistungen erbringt, kann sie diese Dienste und Leistungen aufgrund technischer, rechtlicher oder wirtschaftlicher Änderungen der

Rahmenbedingungen oder Erwägungen ändern oder einstellen oder bislang vergütungsfrei zur Verfügung gestellte Dienste und Leistungen zukünftig gegen Entgelt weiter anbieten.

Die SINOVO health solutions GmbH wird den Kunden unverzüglich informieren, wenn wegen der vorgenannten Gründe die weitere Zurverfügungstellung von freiwilligen, unentgeltlichen Diensten und Leistungen gefährdet ist. SINOVO health solutions GmbH wird bei der Bemessung der Einstellungs- oder Änderungsfrist oder der Vergütung dieser Dienste und Leistungen auf die Belange des Kunden Rücksicht nehmen.

Der Kunde hat das Recht, innerhalb von 14 Tagen nach Ankündigung der Einstellung, Änderung oder Vergütung der freiwilligen Dienste und Leistungen, außerordentlich zu kündigen. Weitere Rechte des Kunden im Zusammenhang mit der Einstellung, Änderung oder Vergütung freiwilliger Dienste und Leistungen sind ausgeschlossen.

### 3. Server-Erreichbarkeit, Sicherheit

a) Serverausfälle aufgrund höherer Gewalt und aufgrund von Ereignissen, die die SINOVO health solutions GmbH nicht zu vertreten hat und die ihre Leistungen wesentlich erschweren oder unmöglich machen – insbesondere Streik, Aussperrung, behördliche Anordnung, Störungen im Bereich der Dienste der Telekom oder im Internet, übermäßige Nutzung anderer Nutzer, Angriffe von Hacker und/oder „Spammern“ usw., berechtigen den Kunden nur dann zu einer Minderung der Vergütung, wenn die Behinderung erheblich ist und über einen nicht unwesentlichen Zeitraum andauert. Der Kunde ist dann berechtigt, die laufenden monatlichen Entgelte und Gebühren bis zum nächsten Kündigungstermin entsprechend zu mindern.

Überschreitet die Behinderung einen unwesentlichen Zeitraum und ist dem Kunden aus diesem Grund eine Fortsetzung des Vertrages bis zum nächsten Kündigungstermin nicht zumutbar, hat er das Recht, den Vertrag außerordentlich und ohne Einhaltung einer Frist zu kündigen. Der Kündigung hat eine Kündigungsandrohung mit Setzen einer angemessenen Frist zur Beseitigung des Kündigungsgrundes vorauszugehen. Weitere Rechte stehen dem Kunden nicht zu, außer im Fall von Vorsatz, grober Fahrlässigkeit oder Verletzung einer wesentlichen Vertragspflicht der SINOVO health solutions GmbH.

b) Die in mylife™ Software Online-Version verfügbaren Daten können nur unter Verwendung der Benutzerkennung und des Kennwortes (Zugangsdaten) abgerufen werden. Der Kunde verpflichtet sich, diese Zugangsdaten streng geheim zu halten und die SINOVO health solutions GmbH unverzüglich zu informieren, sobald er davon Kenntnis erlangt, dass das die Zugangsdaten ganz oder teilweise Dritten bekannt sind. Sollten infolge Verschuldens des Kunden Dritte durch Missbrauch der Zugangsdaten Einfluss auf die gespeicherten Daten genommen werden, wozu auch u. a. deren Änderung, Löschung, das Herunterladen sowie das Weiterleiten zählen, übernimmt SINOVO health solutions GmbH hierfür keine Haftung. SINOVO health solutions GmbH ist in diesem Fall berechtigt, das Benutzerkonto zu sperren und dem Kunden ein neues Kennwort zu erteilen. Dadurch entstehende angemessene Kosten sind vom Kunden zu tragen.

c) Die SINOVO health solutions GmbH weist ausdrücklich darauf hin, dass der Schutz für Datenübertragungen in offenen Netzen, wie dem Internet, nach dem derzeitigen Stand der Technik, nicht umfassend gewährleistet werden kann. Die auf den Servern der SINOVO health solutions GmbH gespeicherten Informationen können aus technischer Sicht unter Umständen auch von anderen Teilnehmern am Internet unbefugt eingesehen und verändert werden. Die SINOVO health solutions GmbH hat ihre Server mit erprobten und verkehrsüblichen Systemen gegen unbefugten Zugriff gesichert. Eine Haftung der SINOVO health solutions GmbH für Eingriffe in den Datenbestand, die trotz der Funktionsfähigkeit der von der SINOVO health solutions GmbH bereitgestellten Systemsicherungen erfolgen, ist ausgeschlossen.

d) Es obliegt dem Kunden bei Veränderungen des Datenbestands eine Datensicherung auf eigenen Speichermedien (Festplatte, Diskette o. ä.) durchzuführen. Insbesondere die in „mylife™ Software Online-Version“ eingespeisten, gesundheitsrelevanten Daten sind auf eigenen Speichermedien zusätzlich zu sichern. Der Kunde ist verpflichtet im Rahmen seiner Kenntnisse und Fähigkeiten, Software vor ihrer Verwendung auf Mangelfreiheit und Verwendbarkeit in der konkreten Situation zu testen, bevor er mit der operativen Nutzung des Programms beginnt. Dies gilt auch für Programme, die der Kunde von der SINOVO health solutions GmbH erhält. Der Kunde hat sich im Zweifel an den technischen Support der SINOVO health solutions GmbH unter +49 6109-500

3909 / info@sinovo.de zu wenden. Der Kunde wird ausdrücklich darauf hingewiesen, dass bereits geringfügige Veränderungen an der Software die Lauffähigkeit und Nutzbarkeit des gesamten Systems beeinflussen können.

e) Die SINOVO health solutions GmbH übernimmt keine Gewähr dafür, dass die mylife™ App oder die hierüber vermittelten Inhalte mit der Hardware und Software des mobilen Endgerätes des Kunden vereinbar sind.

#### **4. Vertragsabschluss, Vertragsbeendigung**

a) Der Vertrag mit der SINOVO health solutions GmbH kommt durch Ausfüllen und Absenden des Online-Formulars unter <https://mylife-software.net/register> durch den Kunden mit Eingang bei der SINOVO health solutions GmbH zustande.

b) Der Vertrag wird auf unbestimmte Zeit geschlossen. Das Vertragsverhältnis kann von beiden Parteien ohne Angabe von Gründen mit einer Frist von 30 Tagen zum Monatsende gekündigt werden.

c) Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

d) Jede Kündigung bedarf zu ihrer Wirksamkeit der Schriftform, welche auch durch Zusendung einer E-Mail gewahrt ist.

e) Die Teilnahme von Ärzten erfordert die Anmeldung als Arzt und die Verifizierung als solcher.

#### **5. Haftung**

Soweit diese AGB keine gesonderten Bestimmungen enthalten, ist die Haftung der SINOVO health solutions GmbH wie nachfolgend geregelt:

a) Die SINOVO health solutions GmbH haftet nicht für Schäden, die durch Fehler, Verzögerungen oder Unterbrechungen in der Übermittlung, bei Störungen der technischen Anlagen, unvollständige Daten, Viren oder in sonstiger Weise bei der Nutzung der mylife™ App entstehen, sofern sie nicht auf Vorsatz und grober Fahrlässigkeit beruhen.

b) Für Schäden haftet die SINOVO health solutions GmbH nur dann, wenn die SINOVO health solutions GmbH oder einer ihrer Erfüllungsgehilfen eine wesentliche Vertragspflicht (Kardinalspflicht) verletzt hat oder der Schaden auf grobe Fahrlässigkeit oder Vorsatz der SINOVO health solutions GmbH oder einer ihrer Mitarbeiter oder Erfüllungsgehilfen zurückzuführen ist. Die Haftung der SINOVO health solutions GmbH für Schäden des Lebens, des Körpers oder der Gesundheit, sowie für Garantien bleibt unberührt.

c) Die Haftung der SINOVO health solutions GmbH ist in den Fällen der Ziff. 5 b) auf den Schaden des Kunden beschränkt, der für die SINOVO health solutions GmbH bei Vertragsschluss vernünftigerweise voraussehbar war.

#### **6. Vergütung**

a) Wird eine Vergütung vereinbart, wird diese 14 Tage nach Rechnungsstellung fällig. Die SINOVO health solutions GmbH kann bei Zahlungsverzug die weitere Bearbeitung des laufenden Auftrages nach ihrer Wahl bis zur Bezahlung zurückstellen oder Vorauszahlungen verlangen.

b) Mangels anderer Vereinbarung gilt die jeweilige Preisliste der SINOVO health solutions GmbH, die über <https://mylife-software.net/tariff> abrufbar ist.

## 7. Widerrufsrecht

### Widerrufsrecht

Sie haben das Recht, innerhalb von vierzehn Tagen ohne Angabe von Gründen einen Vertrag zu widerrufen. Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag des Vertragsschlusses, jedoch nicht bevor Sie diese Belehrung in Textform erhalten haben und nicht bevor Sie von uns entsprechend den Anforderungen des Artikels 246a § 1 Absatz 2 Satz 1 Nummer 1 EGBGB unterrichtet wurden. Um Ihr Widerrufsrecht auszuüben, müssen Sie uns – der SINOVO health solutions GmbH, Casimirstr. 2-4, 60388 Frankfurt/Main, Telefon 06172 3986 – 90, Fax 069 3986 – 91, email [info@sinovo.net](mailto:info@sinovo.net) eine eindeutige Erklärung zukommen lassen (z. B. als Brief per Post, als Faxschreiben oder als E-Mail), dass Sie den Vertrag widerrufen. Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechts vor Ablauf der Widerrufsfrist absenden. Für eine Mitteilung s. auch Anlage 1. (am Ende dieses Dokuments).

## 8. Folgen des Widerrufs

Wenn Sie diesen Vertrag widerrufen, haben wir Ihnen alle Zahlungen, die wir von Ihnen seit Vertragsschluss erhalten haben, unverzüglich und spätestens binnen vierzehn Tagen ab dem Tag zurückzuzahlen, an dem die Mitteilung über Ihren Widerruf dieses Vertrags bei uns eingegangen ist. Für die Rückzahlung verwenden wir dasselbe Zahlungsmittel, das Sie bei der ursprünglichen Transaktion eingesetzt haben, es sei denn, mit Ihnen wurde ausdrücklich etwas anderes vereinbart. Entgelte werden Ihnen im Zusammenhang mit der Rückzahlung in keinem Fall berechnet.

## 9. Schlussbestimmungen

- a) Mündliche Nebenabreden bestehen bei Vertragsschluss nicht.
- b) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Erfüllungsort und Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag, ist bei Verträgen mit Kaufleuten der Sitz der SINOVO health solutions GmbH.
- c) Die SINOVO health solutions GmbH weist darauf hin, dass Sie neben dem ordentlichen Rechtsweg auch die Möglichkeit einer außergerichtlichen Beilegung von Streitigkeiten gemäß Verordnung (EU) Nr. 524/2013 haben. Einzelheiten dazu finden sich in der Verordnung (EU) Nr. 524/2013 und unter der Internetadresse: <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32013R0524>. Die SINOVO health solutions GmbH ist weder verpflichtet, noch dazu bereit, an Streitbelegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Stand: Mai 2018

Anlage 1:

Muster für das Widerrufsformular

Wenn Sie den Vertrag widerrufen wollen, dann füllen Sie bitte dieses Formular aus und senden Sie es zurück:

– An

SINOVO health solutions GmbH  
Casimirstr. 2-4  
60388 Frankfurt am Main  
Deutschland

E-Mail: [info@sinovo.de](mailto:info@sinovo.de)

– Hiermit widerrufe(n) ich/wir (\*) den von mir/uns (\*) abgeschlossenen Vertrag über den Erwerb der mylife™ Software

– Bestellt am (\*)/erhalten am (\*)

– Name des/der Verbraucher(s)

– Anschrift des/der Verbraucher(s)

– Unterschrift des/der Verbraucher(s) (nur bei Mitteilung auf Papier)

– Datum

\_\_\_\_\_  
\_\_\_\_ (\*) Unzutreffendes streichen.

**YPSOMED**





# Datenschutzrichtlinie der SINOVO health solutions GmbH

Die SINOVO health solutions GmbH nimmt den Schutz von personenbezogenen Daten sehr ernst. Wir richten unsere Datenverarbeitung an dem gesetzlichen Ziel aus, nur die für eine sinnvolle und wirtschaftliche Nutzung unseres Angebotes erforderlichen personenbezogenen Daten zu erheben, zu verarbeiten oder zu nutzen.

Nachfolgend erfahren Sie, wann bei der Nutzung unserer Homepage, der mylife-Software und unserer Dienste Daten gespeichert werden und wie wir sie verwenden. Wir haben organisatorische Maßnahmen getroffen, die sicherstellen, dass die Vorschriften über den Datenschutz eingehalten werden.

Falls Sie mit einem Aspekt unserer Datenschutzrichtlinie nicht einverstanden sind, stehen Ihnen ggf. Rechtsansprüche zu, die hier an entsprechender Stelle ebenfalls beschrieben sind.

## Geltungsbereich

In diesen Richtlinien zum Datenschutz beziehen sich „wir“, „unser“, „uns“:

- SINOVO health solutions GmbH, Casimirstr. 2-4, 60388 Frankfurt am Main;
- Sinovo business solutions GmbH, Casimirstr. 2-4, 60388 Frankfurt am Main

## Personenbezogene Daten

SINOVO health solutions GmbH erhebt, verarbeitet und nutzt Ihre personenbezogenen Daten unter Einhaltung der Datenschutzgesetze der Bundesrepublik Deutschland und der Datenschutzbestimmungen der Europäischen Union. Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Unser Online-Angebot ist grundsätzlich ohne die Offenlegung Ihrer Identität nutzbar. Im Falle der Teilnahme an einem unserer personalisierten Dienste werden Sie gesondert nach den für die

Abwicklung der Dienste erforderlichen Daten gefragt. Es unterliegt Ihrer freien Entscheidung, an diesen Diensten teilzunehmen und die entsprechenden Daten einzugeben.

Wir weisen ausdrücklich darauf hin, dass der Schutz für Datenübertragungen in offenen Netzen, wie dem Internet, nach dem derzeitigen Stand der Technik, nicht umfassend gewährleistet werden kann. Die auf den Servern der SINOVO health solutions GmbH oder der Microsoft Cloud gespeicherten Informationen können aus technischer Sicht unter Umständen auch von anderen Teilnehmern am Internet unbefugt eingesehen und verändert werden. Die SINOVO health solutions GmbH oder Microsoft haben ihre Server mit erprobten und verkehrsüblichen Systemen gegen unbefugten Zugriff gesichert.

## Art und Umfang der erfassten Daten und ihrer Verwendung

Beim Aufrufen unserer Website <https://mylife-software.net> (und deren Subdomains) werden durch den auf Ihrem Endgerät zum Einsatz kommenden Browser automatisch Informationen an den Server unserer Website gesendet. Diese Informationen werden temporär in einem sog. Logfile gespeichert. Folgende Informationen werden dabei ohne Ihr Zutun erfasst und bis zur automatisierten Löschung gespeichert:

IP-Adresse des anfragenden Rechners, Datum und Uhrzeit des Zugriffs, Name und URL der abgerufenen Datei, Website, von der aus der Zugriff erfolgt (Referrer-URL), verwendeter Browser und ggf. das Betriebssystem Ihres Rechners sowie der Name Ihres Access-Providers.

Die genannten Daten werden durch uns zu folgenden Zwecken verarbeitet:

- Gewährleistung eines reibungslosen Verbindungsaufbaus der Website,
- Gewährleistung einer komfortablen Nutzung unserer Website,
- Auswertung der Systemsicherheit und -stabilität sowie
- zu weiteren administrativen Zwecken.

Die Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 S. 1 lit. f DSGVO. Unser berechtigtes Interesse folgt aus oben aufgelisteten Zwecken zur Datenerhebung. In keinem Fall verwenden wir die erhobenen Daten zu dem Zweck, Rückschlüsse auf Ihre Person zu ziehen.

Darüber hinaus setzen wir beim Besuch unserer Website Cookies sowie Analysedienste ein. Nähere Erläuterungen dazu erhalten Sie unten.

Auch wenn Sie auf unsere Website zugreifen, erfassen wir bestimmte Daten über Sie. Weitere Informationen dazu finden Sie im Abschnitt Log-Dateien.

Zur Auswertung und zur fortlaufenden Verbesserung der Qualität unseres Internetangebotes nehmen wir statistische Auswertungen der Zugriffe auf unsere Seiten vor. Dies erfolgt teilweise auch durch Verwendung von in den Seiten unseres Angebotes angebrachten Zählgrafiken. Die so gewonnenen Daten sind jedoch strikt

anonymisiert und lassen keine Rückschlüsse auf personenbezogene Daten der Nutzer bzw. auf die Person des Nutzers zu. Ihre Daten werden in keinem Falle zur Erstellung von Nutzerprofilen - gleich welcher Art - verwendet.

Die erhobenen Daten werden für folgende Zwecke genutzt:

- Bereitstellung, Pflege, Verbesserung und Entwicklung relevanter Funktionen, Inhalte und Dienste;
- Erkennung von und Verteidigung gegen betrügerische, missbräuchliche und verbotene Aktivitäten sowie Schutz und Sicherheit unserer Dienste.

Einladungen in der mylife Software Online-Version

Mit der mylife Software können Sie andere Personen zur Mitgliedschaft und zur Besichtigung Ihrer Online-Daten einladen. Die dabei erhobenen personenbezogenen Daten werden ausschließlich für die Einladung verwendet und nicht für andere Zwecke.

## **Schutz und Aufbewahrung von personenbezogenen Daten**

Für den bestmöglichen Schutz Ihrer personenbezogenen Daten nutzt die SINOVO health solutions GmbH bezüglich der von der mylife-Software erhobenen Therapie- und Geräte-Daten die Cloud-Dienste von Microsoft (Windows Azure). Diese Daten werden in Europa gespeichert.

Wir bewahren Ihre Daten nur so lange auf, wie es für die Zwecke notwendig ist, die in dieser Datenschutzrichtlinie dargelegt werden, oder für die Zeit, die Ihr Account bei der SINOVO health solutions GmbH oder Microsoft aktiv ist und es notwendig ist, um die Dienste für Sie bereitzustellen. Wenn Sie nicht mehr wünschen, dass die SINOVO health solutions GmbH Ihre Daten verwendet, um die Dienste für Sie bereitzustellen, können Sie Ihren Account schließen und die SINOVO health solutions GmbH wird die gespeicherten Daten löschen, soweit die SINOVO health solutions GmbH nicht verpflichtet ist, Ihre Daten zur Einhaltung rechtlicher Verpflichtungen oder zur Beilegung von Streitfällen aufzubewahren.

Wenn wir zwei Jahre lang keinen relevanten Kontakt mit Ihnen hatten, werden wir Ihre personenbezogenen Daten aus unseren Systemen löschen, sofern wir nicht in gutem Glauben davon überzeugt sind, dass wir gesetzlich oder aufgrund einer anderen Vorschrift verpflichtet sind, sie aufzubewahren (beispielsweise, weil eine Anfrage in Verbindung mit einem voraussichtlichen Rechtsstreit vorliegt).

### **Weitergabe personenbezogener Daten an sonstige Dritte**

Wir geben keine personenbezogenen Daten an sonstige Dritte weiter. Insbesondere erfolgt keine Weitergabe personenbezogener Daten an Dritte zu Werbezwecken.

## **Weitergabe von Daten**

Eine Übermittlung Ihrer persönlichen Daten an Dritte zu anderen als den im Folgenden aufgeführten Zwecken findet nicht statt.

Wir geben Ihre persönlichen Daten nur an Dritte weiter, wenn:

- Sie Ihre nach Art. 6 Abs. 1 S. 1 lit. a DSGVO ausdrückliche Einwilligung dazu erteilt haben,
- die Weitergabe nach Art. 6 Abs. 1 S. 1 lit. f DSGVO zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist und kein Grund zur Annahme besteht, dass Sie ein überwiegendes schutzwürdiges Interesse an der Nichtweitergabe Ihrer Daten haben,
- für den Fall, dass für die Weitergabe nach Art. 6 Abs. 1 S. 1 lit. c DSGVO eine gesetzliche Verpflichtung besteht, sowie
- dies gesetzlich zulässig und nach Art. 6 Abs. 1 S. 1 lit. b DSGVO für die Abwicklung von Vertragsverhältnissen mit Ihnen erforderlich ist.

Zu Auswertungszwecken können ausschließlich anonymisierte Daten an sonstige Dritte weitergegeben werden. Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.

Sofern Sie weitere personalisierte Dienstleistungen unseres Angebotes nutzen, kann zum Zwecke der Durchführung und Abwicklung der Dienstleistung jedoch die Erhebung personalisierter Daten und deren Weitergabe an Dritte erforderlich sein. Diese Daten werden jedoch nur im für die Auftragsabwicklung erforderlichen Maße gespeichert oder weitergegeben. Dazu ist beim Ausfüllen des jeweiligen Formulars die Abgabe einer ausdrücklichen Einverständniserklärung erforderlich.

Auch Dritte, an die Ihre Daten im Rahmen der Auftragsabwicklung weitergegeben werden, sind im Übrigen an die gesetzlichen Vorschriften für den Umgang mit personenbezogenen Daten gebunden. Soweit wir gesetzlich oder per Gerichtsbeschluss dazu verpflichtet sind oder werden, übermitteln wir Daten im gesetzlich vorgeschriebenen Umfang an die jeweils auskunftsberechtigten Stellen.

## **Recht auf Widerruf, Auskunftserteilung, Löschung und Datenübertragbarkeit**

### **Betroffenenrechte**

Sie haben das Recht:

- gemäß Art. 15 DSGVO Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten zu verlangen. Insbesondere können Sie Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen;
- gemäß Art. 16 DSGVO unverzüglich die Berichtigung unrichtiger oder Vervollständigung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen;
- gemäß Art. 17 DSGVO die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;
- gemäß Art. 18 DSGVO die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von Ihnen bestritten wird, die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen und wir die Daten nicht mehr benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen oder Sie gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung eingelegt haben;
- gemäß Art. 20 DSGVO Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen;
- gemäß Art. 7 Abs. 3 DSGVO Ihre einmal erteilte Einwilligung jederzeit gegenüber uns zu widerrufen. Dies hat zur Folge, dass wir die Datenverarbeitung, die auf dieser Einwilligung beruhte, für die Zukunft nicht mehr fortführen dürfen und

- gemäß Art. 77 DSGVO sich bei einer Aufsichtsbehörde zu beschweren. In der Regel können Sie sich hierfür an die Aufsichtsbehörde Ihres üblichen Aufenthaltsortes oder Arbeitsplatzes oder unseres Kanzleisitzes wenden.

### **Widerspruchsrecht**

Sofern Ihre personenbezogenen Daten auf Grundlage von berechtigten Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO verarbeitet werden, haben Sie das Recht, gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten einzulegen, soweit dafür Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben oder sich der Widerspruch gegen Direktwerbung richtet. Im letzteren Fall haben Sie ein generelles Widerspruchsrecht, das ohne Angabe einer besonderen Situation von uns umgesetzt wird.

Möchten Sie von Ihrem Widerrufs- oder Widerspruchsrecht Gebrauch machen, genügt eine E-Mail an [info@sinovo.de](mailto:info@sinovo.de)

Sie haben das Recht, eine einmal erteilte Einwilligung in die Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft zu widerrufen. Sie können dieses Recht durch einfachen Anruf bei der SINOVO health solutions GmbH ausüben oder uns den Widerruf z. B. schriftlich oder per E-Mail zukommen lassen.

Sie sind jederzeit berechtigt, gegenüber der SINOVO health solutions GmbH um umfangreiche Auskunftserteilung zu den zu Ihrer Person gespeicherten Daten zu ersuchen.

Sie können auch jederzeit gegenüber der SINOVO health solutions GmbH die Berichtigung, Löschung und Sperrung einzelner personenbezogener Daten verlangen.

Falls Sie es wünschen, sind Sie berechtigt, Ihre Daten von uns an einen anderen Verantwortlichen zu übermitteln. Wir werden Sie dabei unterstützen, indem wir Ihre Daten direkt für Sie übermitteln oder indem wir Ihnen eine Kopie in einem üblichen maschinenlesbaren Format zur Verfügung stellen.

### **mylife Software Online-Version – Hinweise für den Datenaustausch mit anderen Personen**

Nutzer/Patienten können mylife Online-Version zum Datenaustausch mit den von ihnen hierfür autorisierten Personen (z.B. Arzt, Vertrauensperson) nutzen. Wir weisen darauf hin, dass die Verbindung von personenbezogenen Daten mit den Gesundheitsdaten technisch möglich sein muss, um Ihrem Arzt die Zuordnung der Daten zu den Patienten zu ermöglichen. Die SINOVO health solutions GmbH wird jedoch personenbezogene Daten mit Gesundheitsdaten nicht derart in Verbindung bringen, dass hierdurch andere als der autorisierte Arzt Gesundheitsdaten bestimmten Personen zuordnen können. Mitarbeiter der SINOVO health solutions GmbH sind entsprechend instruiert und diesen Datenschutzbestimmungen verpflichtet. Keinesfalls werden persönliche oder Gesundheitsdaten an andere sonstige Dritte als den von Ihnen autorisierten Arzt oder andere von Ihnen autorisierte Dritte weitergegeben oder zum Abruf der Daten ermächtigt. Der Zugang zu in mylife Software Online-Version enthaltenen Daten ist nur nach Eingabe der Benutzerkennung und des Kennwortes möglich. Ärzte und Vertrauenspersonen erhalten Zugriff auf die Daten ausschließlich, nachdem Sie Ihren Arzt für den Zugriff autorisiert haben, dieser angemeldet ist und seine Registrierung bei der Anmeldung bestätigt hat. Ärzte und Personen des Vertrauens können die mylife Software zum Datenaustausch mit den Patienten nutzen, von denen sie für den Zugriff auf die Patientendaten autorisiert wurden. Die Autorisierung des Arztes oder eines Dritten kann jederzeit widerrufen

werden. Ab Widerruf werden keine Zugriffe für den jeweiligen Arzt oder Dritten ermöglicht.

## Einsatz von Cookies

Die Dienste von mylife Online-Version benutzen nach Ihrer Anmeldung (mit Benutzernamen und Passwort) Cookies, mit denen Sie während der Dauer Ihres Besuchs identifiziert werden können. Ein Cookie wird auf Ihrem Computer gespeichert. Nach dem Ende der Sitzung verfällt das Cookie automatisch. Sie können dieses Cookie mit der Funktion "Auf diesem Computer automatisch einloggen" für eine automatische Anmeldung dauerhaft speichern. Das Cookie enthält dann Teile Ihrer Anmeldedaten in verschlüsselter Form. Die automatische Anmeldung auf zwei (2) verschiedenen Rechnern ist in diesem Fall allerdings nicht möglich.

## Log-Dateien

Bei jedem Seitenaufruf werden Zugriffsdaten in einer Protokolldatei, dem Server-Log, gespeichert. Der dabei gespeicherte Datensatz enthält die folgenden Daten:

- Ihre IP-Adresse (durch die Ihr Computer eindeutig identifiziert werden kann),
- den Remote Host (Name und IP-Adresse des Rechners, der die Seite anfordert),
- die Uhrzeit, den Status, die übertragene Datenmenge sowie die Internetseite, von der Sie auf die angeforderte Seite gekommen sind (Referrer), sowie
- die Produkt- und Versionsinformationen des verwendeten Browsers (User-Agent).

SINOVO health solutions GmbH benutzt hierfür das standardisierte Logfile-Format des Webservers. SINOVO health solutions GmbH verwendet die Protokolldaten (Logs) anonymisiert, also ohne Zuordnung oder Hinweise auf Ihre Person, für statistische Auswertungen. SINOVO health solutions GmbH kann so z.B. erfahren, an welchen Tagen und zu welchen Uhrzeiten die Angebote von mylife Online-Version besonders beliebt sind und wie viel Datenvolumen auf den SINOVO-Websites erzeugt wird. Zudem kann SINOVO health solutions GmbH durch die Log-Dateien mögliche Fehler erkennen, z.B. fehlerhafte Links oder Programmfehler, und die Log-Dateien damit für die Weiterentwicklung der mylife Online-Version Websites verwenden. SINOVO health solutions GmbH verknüpft die im Server-Log gespeicherten Seitenabrufe und Nutzungen nicht mit einzelnen Personen. SINOVO health solutions GmbH behält sich jedoch vor, die Log-Dateien nachträglich über die letzte bekannte IP-Adresse von solchen Nutzern zu überprüfen, bei denen aufgrund bestimmter Tatsachen der Verdacht besteht, dass diese die mylife Online-Version Websites und/oder die mylife Dienste gesetzes- oder vertragswidrig nutzen. Dies dient sowohl dem Schutz der mylife-Mitglieder, der Sicherheit der SINOVO-Mitgliederdaten, als auch den SINOVO-Websites und den mylife-Diensten.

Die Installation der Cookies kann von Ihnen durch eine entsprechende Einstellung Ihres Browsers verhindert werden. Wenn eine entsprechende Browsereinstellung genutzt wird, werden Cookies nicht gespeichert. Es kann dazu kommen, dass unter Umständen nicht alle Funktionen der mylife Software Online-Version genutzt werden können.

## Kinder unter 18 Jahren

Eine Teilnahme an mylife-Online Diensten ist ausschließlich volljährigen Personen vorbehalten. Eltern oder Aufsichtsberechtigte sind für den Schutz der Privatsphäre

ihrer Kinder verantwortlich.

Personen unter 18 Jahren sollten ohne Zustimmung der Eltern oder Erziehungsberechtigten keine personenbezogenen Daten an uns übermitteln. Wir fordern keine personenbezogenen Daten von Kindern an, sammeln und speichern diese nicht und geben sie auch nicht an Dritte weiter.

### **Links zu anderen Websites**

Soweit unsere Internetseiten Links zu den Angeboten anderer Diensteanbieter enthalten, können wir nicht garantieren und keine Haftung dafür übernehmen, dass auch diese Internetseiten den gesetzlichen Bestimmungen entsprechen. Bitte informieren Sie sich auf den entsprechenden Seiten mit Hilfe der Datenschutzerklärung des jeweiligen Anbieters über die jeweils gültigen Datenschutzstandards.

### **Recht auf Beschwerde bei einer Aufsichtsbehörde**

Unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs steht Ihnen das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, zu, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt.

Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Art. 78 DSGVO.

Die für die SINOVO health solutions GmbH zuständige Aufsichtsbehörde ist der Hessische Datenschutzbeauftragte.

### **Name und Anschrift des Verantwortlichen**

Der Verantwortliche im Sinne der Datenschutz-Grundverordnung ist die:

SINOVO health solutions GmbH  
Casimirstr. 2-4  
60388 Frankfurt am Main  
Deutschland

Tel.: +49 61 09 500 39 00

E-Mail: [info@sinovo.de](mailto:info@sinovo.de)  
Website: [www.sinovo.de](http://www.sinovo.de)



Name und Anschrift des Datenschutzbeauftragten:

Der Datenschutzbeauftragte des Verantwortlichen ist:

Katja Deisenroth  
Casimirstr. 2-4  
60388 Frankfurt am Main  
Deutschland

Tel.: +49 61 09 500 39 47  
E-Mail: [datenschutz@sinovo.de](mailto:datenschutz@sinovo.de)

## Änderungen

Diese Hinweise unterliegen der jeweiligen Rechtslage und können daher Anpassungen erforderlich machen. Für Fragen, Anregungen oder Kommentare wenden Sie sich bitte per E-Mail an [info@sinovo.net](mailto:info@sinovo.net)

Die jeweils aktuelle Datenschutzerklärung kann jederzeit auf der Website unter <https://mylife-software.net/privacy> von Ihnen abgerufen und ausgedruckt werden.

Stand: Mai 2018

**YPSOMED**

## BVKD-Geschäftsstelle

---

**Von:** WILHELM, Isabel <Isabel.wilhelm@vitalaire.de>  
**Gesendet:** Donnerstag, 8. April 2021 09:14  
**An:** info@die-diabetes-kliniken.de  
**Cc:** BRAUNE, Steffen  
**Betreff:** Ihre Anfrage vom 5.3.21  
**Anlagen:** BVKD Glooko (1).pdf; Annual Diabetes Report One Pager 2020 (1) (1).pdf; T309v7C Booking form diasend® Start and Premium (DE) (3).pdf; M0296v7A Trial Agreement\_DE (5) (1).pdf

**Kennzeichnung:** Zur Nachverfolgung  
**Kennzeichnungsstatus:** Gekennzeichnet

Sehr geehrter Herr Dr. Jannaschk,

ich beziehe mich auf Ihr postalisches Schreiben vom 5.3.21.

Wir haben Ihre Fragen an die Firma Diasend/Glooko weitergeleitet und anhängende Infos erhalten.

Sollten Sie noch weitere Fragen haben, zögern Sie nicht uns zu kontaktieren.

Mit freundlichen Grüßen

i.A. Dr. Isabel Wilhelm  
Dipl. Biol. / MBA  
Business Unit Manager Diabetes



**VitalAire GmbH**  
Hauptniederlassung Hamburg  
Bornbarch 2  
22848 Norderstedt  
Tel +49 160 903 568 15  
Fax +49 (0) 40 / 3 20 91 – 5163

[Isabel.Wilhelm@vitalaire.de](mailto:Isabel.Wilhelm@vitalaire.de)

Die gesetzlichen Pflichtangaben finden Sie unter:  
<https://www.vitalaire.de/impressum>

Göteborg 2021-03-30

## **Nachfolgend die Antworten auf die Fragen des BVKD**

**1. Auf welcher Rechtsgrundlage erfolgen die zur Nutzung der von Ihnen angebotenen Cloud-Lösung (im Folgenden: "Produkt") erforderlichen Datenverarbeitungsverträge?**

### **Glooko AB fungiert als Controller**

Glooko fungiert als Controller für seine eigenen Prozesse, wenn es um die Zwecke und Mittel der Prozesse geht. Beispiele dafür, wann Glooko als Controller fungiert, sind - wenn Patienten sich auf ihrem eigenen Konto (Self Registered Patient Account) anmelden, z. beim Hochladen von Daten von zu Hause über die diasend-Uploader-Software.

Bei Prozessen, bei denen Glooko als Controller fungiert, hält sich Glooko stets an die Datenschutzerklärung. Die Datenschutzerklärung gilt nicht für den Fall, dass Glooko als Prozessor fungiert (siehe Abschnitt 14 der Datenschutzerklärung).

Glooko führt verschiedene Verarbeitungsaktivitäten auf der Grundlage unterschiedlicher Rechtsgrundlagen durch. Im Allgemeinen ist die Rechtsgrundlage für die Bereitstellung von Diasend für Benutzer die Zustimmung und die ausdrückliche Zustimmung (Artikel 6.1 (a) und 9.2 (a) der DSGVO).

### **Glooko AB fungiert als Datenverarbeiter**

Als Datenverarbeiter wird Glooko immer die geltenden Datenschutzbestimmungen (z. B. die DSGVO) und die geltenden Datenverarbeitungsvereinbarungen einhalten.

Glooko fungiert als Datenverarbeiter bei der Bereitstellung der Services für professionelle Kunden wie Kliniken und

- wenn Patienten ihre Gerätedaten in einer Klinik über den Transmitter hochladen,
- wenn Kliniken Patientenkonten im Klinikkonto erstellen (In-Klinikpatientenkonto)

Wenn Glooko seine Dienstleistungen für kommerzielle Parteien wie Kliniken erbringt, ist es Sache der Kliniken, über Rechtsgrundlagen zu entscheiden, da Glooko als Verarbeiter im Namen der Klinik als Controller fungiert.

### **Glooko AB**

Nellikevägen 20B  
412 63 Göteborg, Sweden  
+46 (0)31 762 88 88

## **2. Erfolgt die Datenverarbeitung ausschließlich innerhalb der EU?**

Ja, die Lösung wird in Irland gehostet, und andere Verarbeitungsaktivitäten wie Kundensupport und Fehlersuche werden von Glooko-Mitarbeitern in Schweden durchgeführt.

## **3. Ist für die mit der Nutzung des Produkts verbundenen Datenübermittlungs- und Verarbeitungsvorgänge eine Einwilligung der Patienten erforderlich?**

Ja, siehe unter 1.

## **4. Ist die Nutzung Ihrer Cloud- Lösung auf Basis eines Auftragsverarbeitungsvertrags (gem. Art. 28 DSGVO) rechtlich unproblematisch möglich?**

Ja, ein Auftragsverarbeitungsvertrag gemäß Artikel 28 der DSGVO (einschließlich diasendspezifischer Klarstellungen) befindet sich in den AGB, die sich hier befinden: [https://docs.diasend.com/docs/gtc\\_clinic.pdf](https://docs.diasend.com/docs/gtc_clinic.pdf).

## **5. Werden mit dem Produkt verwaltete Patientendaten und / oder hieraus abgeleitete oder anonymisierte Daten von Ihnen oder Dritten ganz oder teilweise für eigene Zwecke genutzt, beispielsweise zu statistischen Zwecken, zur Produktverbesserung oder Forschung? Falls ja, bitte angeben, welche Daten von wem in welcher Form und für welche Zwecke verarbeitet werden.**

Ja, von Glooko. Der Zweck und das Format sind z.B. durch Erstellung aggregierter Jahresberichte siehe beigefügten Bericht für 2020.

## **6. Welche datenschutzrechtlichen Organisationsmaßnahmen muss der Anwender in Bezug auf das Produkt vornehmen, damit das Produkt datenschutzkonform eingesetzt werden kann?**

Dies hängt davon ab, wer der Benutzer ist und welche Anforderungen er hat. diasend® wurde mit ausreichenden Funktionen entwickelt, um ein hohes Maß an Datenschutz zu gewährleisten.

## **7. Wie ist garantiert, dass die mit dem Produkt verwalteten Daten für die Dauer der jeweils geltenden gesetzlich vorgeschriebenen Aufbewahrungsfristen zugänglich sind?**

Dies ist nicht garantiert und es liegt an den Kliniken, die Daten herunterzuladen und bei Bedarf zu speichern.

**8. Ist für die Nutzung des Produkts die dauerhafte Einwilligung des Anwenders und / oder des jeweiligen Patienten in Nutzungsbestimmungen erforderlich? Falls ja: bitte senden Sie uns die aktuelle Fassung der Nutzungsbedingungen.**

Die Nutzungsbedingungen finden Sie hier: <https://docs.diasend.com/docs/gtc.pdf>  
Bei der Registrierung in selbst registrierten Patientenkonten akzeptieren die Benutzer sowohl die Bedingungen als auch die Zustimmung zur Verarbeitung ihrer persönlichen Daten durch Glooko gemäß der Datenschutzerklärung von Glooko, die sich hier befindet: <https://www.glooko.com/privacy/>

**9. Welche Kosten fallen für die Nutzung des Produktes an?**

Es gibt zwei verschiedene Preismodelle. Welches sich für Sie eignet hängt vor allem von der Größe Ihrer Klinik und dementsprechend der Anzahl der Patienten und des Pflegepersonals ab.

Hier ein kurzer Überblick:

1. diasend® Start - €100 pro Jahr (ohne USt.):

- Insulinpaket
- CGM-Paket
- < 1000 Patienten
- 1 Transmitter
- USB-Hub und Aufbewahrungsbox für Kabel
- Werbenachrichten können vorkommen

2. diasend® Pro - €1400 pro Jahr (ohne USt.)

- Insulinpaket
- CGM-Paket
- Unbegrenzte Anzahl von Patienten
- 1-3 Transmitter
- Schwangerschaftspaket
- USB-Hub und Aufbewahrungsbox für Kabel
- keine Werbenachrichten

Die ausführliche Preisliste entnehmen Sie bitte dem PDF Dokument im Anhang.

Wir bieten derzeit auch die Möglichkeit an, das diasend® System bis zu sechs Monate im Rahmen eines Probevertrags kostenfrei zu testen. Bitte beachten Sie, dass auch bei einem Probevertrag Versandkosten für den Transmitter in Höhe von 70 EURO einmalig in Rechnung gestellt werden.

**10. Ist die komplette Nutzung des Produkts ohne Installation, d.h. allein per Internet-Browser möglich oder müssen zusätzlich Komponenten wie Treiber, Uploadprogramme oder Dienste lokal installiert werden? Falls eine Installation erforderlich ist: was genau muss installiert werden und welche administrativen Rechte sind dazu erforderlich? Können sich hierdurch Risiken in Bezug auf die IT-Sicherheit der Klinik ergeben?**

Es ist keine Installation notwendig.

Bei weiteren Fragen können Sie sich gerne an mich wenden.

Mit freundlichen Grüßen

Rosemarie Ingblad  
Senior Customer Support Specialist

Glooko AB  
Nellickevägen 20  
412 63 Göteborg  
Tel: +46 793 41 21 57

Die in diesem Dokument enthaltenen Informationen dienen ausschließlich der Information und Transparenz zum Datum der Veröffentlichung. Glooko übernimmt keine Verantwortung oder Haftung im Zusammenhang mit der Verwendung der in diesem Dokument enthaltenen Informationen. Die Beziehungen von Glooko zu Kunden, Partnern usw. werden in den geltenden Vereinbarungen geregelt, die ggf. Vorrang vor diesem Dokument haben. Die in diesem Dokument enthaltenen Informationen stellen keine Beratung durch Glooko in irgendeiner Form dar, und bei Bedarf sollten Sie sich extern beraten lassen.

## BVKD-Geschäftsstelle

---

**Von:** Dr. Dominik Greim <d.greim@eyedsec.de>  
**Gesendet:** Dienstag, 13. April 2021 09:59  
**An:** 'geschaeftsstelle@die-diabetes-kliniken.de'  
**Cc:** Richard Laqua; Dipl.-Biol. Monique Seyfarth  
**Betreff:** AW: Fragen zu datenschutzrechtlichen Bedingungen (IME-DC)

Sehr geehrter Herr Jannaschk,

im Auftrag von Herrn Laqua und nach Rücksprache mit der Geschäftsführung und der Leitung des Gesundheitsmanagements der IME-DC GmbH kann ich ihre Fragen wie folgt beantworten:

1. Da es sich bei Gesundheitsdaten um hochsensible Informationen privater Personen handelt und der IME-DC Datenschutz sehr am Herzen liegt bietet diese aktuell keine Produkte mit Cloud-Anbindung an. Da daher keine Verarbeitung durch die IME-DC stattfindet ist auch keine Rechtsgrundlage notwendig.
2. Grundsätzlich finden alle Verarbeitungen personenbezogener Daten durch die IME-DC als Verantwortlicher innerhalb der EU statt.
3. Da im Rahmen der Nutzung der Produkte der IME-DC diese nicht als Verantwortlicher im Sinne der DSGVO auftritt, ist keine Rechtsgrundlage notwendig. Aus unserer Sicht ist bei der Nutzung im Klinikbetrieb jedoch eine Nutzung auf Basis von Art. 9 lit. h unter den in Art. 9 Abs. 3 genannten Bedingungen durch den Verantwortlichen möglich.
4. Da keine Cloud-Lösung angeboten wird, erfolgt auch keine Verarbeitung im Auftrag. Daher wird kein AVV gem. Art. 28 benötigt.
5. Nein, s. 1.
6. Es müssen m.E. keine, über die in der DSGVO & BDSG genannten Pflichten hinausgehenden, datenschutzrechtlichen Organisationsmaßnahmen ergriffen werden.
7. Es werden keine Daten verwaltet (s. 1.).
8. Eine Einwilligung in Nutzungsbedingungen ist nicht notwendig.
9. Falls Interesse an Produkten ohne Cloud Anwendung besteht kontaktieren Sie bitte die IME-DC direkt um Produktpreise zu erfragen.
10. Für die Nutzung der Produktreihe DANA Diabecare R und Diabecare RS der *SOOIL* Development Co. Ltd., die durch die IME-DC vertrieben wird, wird die Installation einer App für Mobilbetriebssysteme vorausgesetzt. Auch hier erfolgt die Speicherung von Daten ausschließlich lokal. Die App benötigt darüber hinaus Zugriff auf die Bluetooth Schnittstelle, da über diese mit den Insulinpumpen kommuniziert wird. Aus Sicht der IT-Sicherheit sollte die Nutzung von Mobilgeräten durch eine Nutzungs- & Sicherheitsrichtlinie in Anlehnung an die Anlage 2 Nr. 8 der IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (nach §75b SGB V) geregelt werden. Darüber hinaus bietet sich eine generelle Richtlinie für die Bereitstellung von Mobilgeräten im Praxisbetrieb gem. der Anlage 3 Nr. 1 KBV IT-Sicherheitsrichtlinie an. Über die Risiken, die mit dem Einsatz von Lösungen von Drittanbietern grundsätzlich einhergehen, besteht aus unserer Sicht kein gesondertes Risiko durch den Einsatz der App.

Ich hoffe ich konnte Ihre Fragen zu Ihrer Zufriedenheit beantworten, bei weiteren Fragen oder Anmerkungen stehe ich jederzeit zur Verfügung.

mit freundlichen Grüßen

**Dr. Dominik Greim**

*Datenschutz & IT-Sicherheitsberater*

EMAIL [d.greim@eyedsec.de](mailto:d.greim@eyedsec.de)

MOBIL +49 151 448 266 65

EYEDSEC - INFORMATION SECURITY GMBH

Friedrichstr. 25 / 95444 Bayreuth

Internet: [www.eyedsec.de](http://www.eyedsec.de)

Tel: 0921 23059936

Fax: 0921 15082070

eyeDsec - Information Security GmbH/ Geschäftsleitung: Matthias Mühlhaus, Richard Laqua/ Sitz in Bayreuth/ Amtsgericht Bayreuth/ HRB 5841  
Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Mail ist nicht gestattet. This e-mail may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

---

**Von:** BVKD-Geschäftsstelle <[geschaefsstelle@die-diabetes-kliniken.de](mailto:geschaefsstelle@die-diabetes-kliniken.de)>

**Gesendet:** Freitag, 26. März 2021 13:30

**An:** Richard Laqua <[r.laqua@eyedsec.de](mailto:r.laqua@eyedsec.de)>

**Betreff:** AW: Fragen zu datenschutzrechtlichen Bedingungen

Sehr geehrter Herr Laqua,

zunächst vielen Dank für Ihre Rückmeldung.

Wir beabsichtigen, auf dem Diabetes-Kongress am 12.05.2021 über die Thematik zu berichten. Daher müsste es ausreichen, wenn sie uns in der 15. KW eine Antwort zukommen lassen.

Vielen Dank und freundliche Grüße

Klaus-Dieter Jannaschk  
Bundesverband Klinischer Diabetes-Einrichtungen  
DIE Diabetes-Kliniken e.V.  
Bundes-Geschäftsstelle  
Kirchberg 21  
37431 Bad Lauterberg

Tel: 05524/ 81218

Fax: 05524/ 81398

E-Mail: [geschaefsstelle@bvkd.de](mailto:geschaefsstelle@bvkd.de)

Internet: [www.bvkd.de](http://www.bvkd.de)



**[Hier geht es zu unserer neuen Image-Broschüre ...](#)**

---

**Von:** Richard Laqua <[r.laqua@eyedsec.de](mailto:r.laqua@eyedsec.de)>

**Gesendet:** Freitag, 26. März 2021 12:38

**An:** 'info@die-diabetes-kliniken.de' <[info@die-diabetes-kliniken.de](mailto:info@die-diabetes-kliniken.de)>

**Cc:** Dr. Dominik Greim <[d.greim@eyedsec.de](mailto:d.greim@eyedsec.de)>

**Betreff:** Fragen zu datenschutzrechtlichen Bedingungen

Sehr geehrter Herr Jannaschk,

vielen Dank für Ihr Interesse an den Produkten von der IME-DC GmbH und entschuldigen Sie bitte die verzögerte Rückmeldung.

Gerne werde ich Ihrer Fragen so ausführlich wie möglich beantworten. Die Beantwortung werde ich Ihnen jedoch vermutlich erst in KW15 zusenden können.

Ich hoffe dies ist für Sie noch ausreichend.

Sollten Sie vorab Fragen oder Anmerkungen haben, können Sie mich gerne auch jederzeit direkt kontaktieren.



Vielen Dank

Herzliche Grüße

**Richard Laqua**

*Geschäftsführer; ISB & DSB*

EMAIL [r.laqua@eyeDsec.de](mailto:r.laqua@eyeDsec.de)

MOBIL [+49 160 924 362 55](tel:+4916092436255)

EYEDSEC - INFORMATION SECURITY GMBH

[Friedrichstr. 25 / 95444](#) Bayreuth

Internet: [www.eyeDsec.de](http://www.eyeDsec.de)

Tel: [0921 23059935](tel:092123059935)

Fax: [0921 23059937](tel:092123059937)

eyeDsec - Information Security GmbH/ Geschäftsleitung: Matthias Mühlhaus, Richard Laqua/ Sitz in Bayreuth/  
Amtsgericht Bayreuth/ HRB 5841

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Mail ist nicht gestattet. This e-mail may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

# Zweite Anfrage Pharma-Unternehmen

## Angefragte Unternehmen

Medtronic

Dexcom

Roche

Menarini

Ypsomed

VitalAire/Tandem

Sooil/IME-DE

BVKD e. V. · Kirchberg 21 · 37431 Bad Lauterberg im Harz

XXXXX

Bundes-Geschäftsstelle  
Kirchberg 21  
37431 Bad Lauterberg

Telefon 05524 / 81 218  
Telefax 05524 / 81 398

info@die-diabetes-kliniken.de  
www.die-diabetes-kliniken.de

Bad Lauterberg, 18. November 2021

## Unsere Anfrage zum Datenschutz

Sehr geehrte ...,

wir kommen zurück auf unsere Anfrage zum Datenschutz vom 05.03.2021 und bedanken uns zunächst nochmals herzlich für Ihre Rückantwort.

Zwischenzeitlich konnten wir nun alle Stellungnahmen der angeschriebenen Anbieter sichten. Leider müssen wir feststellen, dass die Antworten einiger Hersteller sich nicht mit der unlängst veröffentlichten Rechtsauffassung der deutschen Datenschutzbehörden decken. Manche Ausführungen stimmen auch nicht mit anderslautenden Verlautbarungen in Werbung und Produktunterlagen überein.

Vor diesem Hintergrund beabsichtigen wir, die erhaltenen Antworten einer juristischen Prüfung zuzuführen sowie gegebenenfalls den Datenschutzbehörden vorzulegen, damit wir abschließend unseren Mitgliedern rechtssichere Empfehlungen geben können.

Wir gehen davon aus, dass eine solche Klärung auch in Ihrem Interesse ist. Daher bitten wir um die Beantwortung der nachfolgenden, weiteren Fragen zu jedem Ihrer nachstehenden Hilfsmittel:

XXXXXXXXXXXXXXXXXXXX

**Frage 1:**

Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung, Ereignisse, Alarme, manuelle Eingaben, Basalratenprogrammierung, ...) für ein computergestütztes Diabetes-Datenmanagement genutzt werden, ohne dass hierzu diese Daten an Dritte übermittelt werden (müssen)?

Falls ja: Bitte beschreiben Sie die Möglichkeiten, die der Klinik zu Verfügung stehen. Bitte teilen Sie auch mit, wenn und inwieweit sich nicht alle mit dem Hilfsmittel erhobenen Daten auf diese Weise nutzen lassen.

**Frage 2:**

Wenn der Patient keine Einwilligung zur Datenverarbeitung gemäß den Nutzungsbedingungen der von Ihnen vorgesehenen Cloudlösung(en) erteilen will oder seine Einwilligung später widerruft: Wie können die mit dem Hilfsmittel erhobenen Daten dann weiterhin - über die bloße Möglichkeit zum Ablesen vom Gerätedisplay hinausgehend – im Rahmen eines computergestützten Datenmanagements von der Klinik zur Behandlung genutzt werden, so dass die fehlende Einwilligung zur Datenverarbeitung nicht zu Nachteilen bezüglich der Therapie- und Behandlungsqualität führen muss?

**Frage 3:**

Im klinischen Behandlungsalltag ist sicherzustellen, dass u.a. die Pflichten aus Art. 5 DSGVO (Datenminimierung, Zweckbindung) eingehalten werden und die Vorgaben aus Art. 23 DSGVO erfüllt sind. Zahlreiche Kliniken unterliegen auch dem Anwendungsbereich des BSI-Gesetzes und müssen jede unnötige Schwächung der klinischen IT-Strukturen vermeiden. Vor diesem Hintergrund bevorzugen manche Kliniken anstelle einer cloudbasierten Lösung den Einsatz marktgängiger lokaler Lösungen zum Diabetes-Datenmanagement, die keine Internetverbindung erfordern und die mit zahlreichen Messgeräten bzw. Insulinpumpen unterschiedlicher Hersteller kompatibel sind.

Mit welchen der offline-basierten Datenmanagement-Lösungen anderer Anbieter können die Daten aus dem Hilfsmittel eingelesen werden?

Wir bedanken uns ganz herzlich für Ihre zeitnahe Rückantwort, diese benötigen wir bitte

bis spätestens 30.10.2021.

Für Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

  
Klaus-Dieter Jannaschk  
Geschäftsstellenleiter

# Antwortschreiben der angefragten Unternehmen

Von folgenden Unternehmen liegen Antwortschreiben vor

1. Dexcom
2. Roche
3. Menarini
4. Ypsomed
5. Sooil/IME-DE

## **B) Ihre Fragen**

### **1) Frage 1:**

Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung, Ereignisse, Alarme, manuelle Eingaben, Basalratenprogrammierung, ...) für ein computergestütztes Diabetes-Datenmanagement genutzt werden, ohne dass hierzu diese Daten an Dritte übermittelt werden (müssen)?

Falls ja: Bitte beschreiben Sie die Möglichkeiten, die der Klinik zu Verfügung stehen. Bitte teilen Sie auch mit, wenn und inwieweit sich nicht alle mit dem Hilfsmittel erhobenen Daten auf diese Weise nutzen lassen.

### **Antwort Dexcom:**

Zunächst einmal war es bei der Entwicklung des CGM-Systems von Dexcom nie das Ziel, die Übertragung von Patientendaten in eine offline-Computer-basierte Datenverwaltung für den lokalen Bereich zu ermöglichen. Die Dexcom CLARITY-Software als Cloud-Service von Dexcom wurde als wichtiger Bestandteil eines komfortablen Diabetes-Management-Systems konzipiert, und zwar aus Effizienzgründen, die naturgemäß mit der Nutzung von Cloud-Services verbunden sind, und im Einklang mit der Bereitstellung innovativer Gesundheitsdienstleistungen für Patienten in einem zunehmend digitalisierten Gesundheitssystem (siehe auch die Aussagen der deutschen „Entscheider“ unter 1) oben).

Dennoch gibt es Möglichkeiten, die Weitergabe der Daten an Dritte zu vermeiden, auch wenn dies die von den CLARITY-Cloud-Diensten angebotenen Funktionen einschränkt (weil das CGM-System von Dexcom als Cloud-System konzipiert ist, um als innovatives Instrument Patienten effektive Vorteile zu erbringen).

Wenn Patienten ihre Daten mit niemandem teilen möchten (z. B. Dexcom, Follower), können sie eine separate Hardware, den Dexcom-Empfänger, verwenden oder ein Mobiltelefon wie einen Empfänger nutzen, ohne dass Patienten ihre Einwilligung dazu erteilen müssen, z. B. in Verbindung mit der Weitergabe ihrer Daten an Follower oder der Nutzung der CLARITY-Software. Der Empfänger, der Sensor und der Sender sind die zentralen Elemente des Dexcom-Systems zur kontinuierlichen Blutzuckermessung. Der Empfänger empfängt die vom Sender übertragenen Glukosewerte alle fünf Minuten und speichert die empfangenen Werte der letzten 30 Tage. Aufgrund der Größe des Empfängers und seines Displays ist es nicht möglich, die Glukosedaten, die vor mehr als 24 Stunden gemessen wurden, zu überprüfen. Die Möglichkeit, längere Zeiträume abzurufen, war auch kein Ziel bei der Entwicklung des Geräts. Die Anzeige der aktuellen Messung, insbesondere für die letzten 60 Minuten, ist die Kernfunktion in einer Diabetesbehandlung, die dazu dient, akute Gefahren und Langzeitschäden zu vermeiden.

Wenn jedoch die Dexcom CLARITY Software, ein retrospektives Therapiemanagement-Tool, das Ihnen Zugang zu Ihren historischen Blutzuckermessungen ermöglicht, verwendet werden soll, besteht schließlich auch die Möglichkeit der anonymen Nutzung dieser Software:

Wenn eine medizinische Fachkraft, die die CLARITY Clinic Software verwendet, Empfängerdaten vom Empfänger des Patienten über eine physische USB-Verbindung an die CLARITY Clinic Software überträgt, hat die medizinische Fachkraft die Möglichkeit, die Patientendaten anonymisiert hochzuladen. In diesem Fall werden die Daten nur für die jeweilige Sitzung gelesen und ausgewertet. Sobald die medizinische Fachkraft zur Patientenliste zurückkehrt, kann sie nicht mehr auf die Patientendaten zugreifen.

## **2) Frage 2:**

Wenn der Patient keine Einwilligung zur Datenverarbeitung gemäß den Nutzungsbedingungen der von Ihnen vorgesehenen Cloudlösung(en) erteilen will oder seine Einwilligung später widerruft: Wie können die mit dem Hilfsmittel erhobenen Daten dann weiterhin - über die bloße Möglichkeit zum Ablesen vom Gerätedisplay hinausgehend – im Rahmen eines computergestützten Datenmanagements von der Klinik zur Behandlung genutzt werden, so dass die fehlende Einwilligung zur Datenverarbeitung nicht zu Nachteilen bezüglich der Therapie- und Behandlungsqualität führen muss?

### **Antwort Dexcom:**

Siehe oben. Die Dexcom CLARITY Software als Cloud-Service von Dexcom wurde entwickelt, um ein wichtiger Teil eines komfortablen Diabetes-Management-Systems zu sein, im Gegensatz zu einem CGM-System, das die Übertragung von Patientendaten an lokale Systeme von Gesundheitsversorgern ermöglicht.

Neben der Möglichkeit, Daten vom Gerätedisplay abzulesen (oder auf lokal gespeicherte CGM-Daten in der App zuzugreifen), ermöglicht die Dexcom CLARITY Software auch die anonyme Nutzung dieser Software.

## **3) Frage 3:**

Im klinischen Behandlungsalltag ist sicherzustellen, dass u.a. die Pflichten aus Art. 5 DSGVO (Datenminimierung, Zweckbindung) eingehalten werden und die Vorgaben aus Art. 23 DSGVO erfüllt sind. Zahlreiche Kliniken unterliegen auch dem Anwendungsbereich des BSI-Gesetzes und müssen jede unnötige Schwächung der klinischen IT-Strukturen vermeiden. Vor diesem Hintergrund bevorzugen manche Kliniken anstelle einer cloudbasierten Lösung den Einsatz marktgängiger lokaler Lösungen zum Diabetes-Datenmanagement, die keine Internetverbindung erfordern und die mit zahlreichen Messgeräten bzw. Insulinpumpen unterschiedlicher Hersteller kompatibel sind.

Mit welchen der offline-basierten Datenmanagement-Lösungen anderer Anbieter können die Daten aus dem Hilfsmittel eingelesen werden?

### **Antwort Dexcom:**

Wie bereits erwähnt, war das CGM-System von Dexcom als Cloud-Service generell nicht für die Übertragung von Patientendaten auf lokale Systeme von Gesundheitsversorgern konzipiert.

Neben den oben beschriebenen Möglichkeiten (Auslesen der CGM-Daten aus dem Gerätedisplay, lokaler Zugriff in der App oder anonyme Nutzung von CLARITY) sind die Produkte von Dexcom jedoch auch interoperabel im Sinne von Industriestandards, so dass unsere Nutzer verschiedene alternative Lösungen (mit oder ohne Cloud-Nutzung) nutzen können, die von externen Anbietern angeboten und betrieben werden. Derzeit gibt es eine Reihe solcher externer Softwarelösungen, darunter u.a. mySugr, MyFitnessPal, Carbs & Cals, myDiabetes, Gluco-Check, Diabetik, DiabetesGuru, Glucose Buddy, etc. Sie können diese bequem mit dem Dexcom rtCGM-System verwenden, da es keine prinzipiellen Unterschiede in der Anwendung zwischen Dexcom und solchen externen Softwarelösungen gibt und, wie bereits erwähnt, die Produkte von Dexcom gemäß Industriestandards interoperabel sind.

Durch die Zusammenarbeit mit Glooko/diasend bietet Dexcom die Möglichkeit, mit Hilfe einer medizinisch geschulten Person eine Langzeitanalyse durchzuführen, ohne dass eine Verbindung zur Dexcom-Cloud erforderlich ist. Zu diesem Zweck können Patienten den Glooko-Sender in der Praxis ihres Diabetologen verwenden. So können Patienten ihren Empfänger über USB mit dem Glooko-Sender verbinden und die Daten direkt vom Empfänger herunterladen, ohne eine Verbindung zur Dexcom-Cloud herstellen zu müssen. So können sie wählen, wo und wie Ihre Daten heruntergeladen werden (weitere Einzelheiten finden Sie in der Bedienungsanleitung des Glooko-Senders - für Glooko-Nutzer und in der Gebrauchsanweisung - für diasend-Nutzer). Die Nutzung von Glooko/diasend setzt jedoch voraus, dass Patienten/Praxen online ein Konto bei Glooko/diasend eröffnen, um auf die Daten zugreifen zu können.

Neben der Glooko/diasend-Lösung ermöglicht Dexcom auch die Übertragung von CGM-Daten an die Apple Health App und Samsung Health App. Es ist möglich, Daten mit Apple Health und Samsung Health zu teilen, ohne die Dexcom-Cloud zu nutzen oder mit Dexcom zu teilen. Die von Apple Health und Samsung Health empfangenen Daten werden mit einer dreistündigen Verzögerung über die Dexcom-API übertragen.

Ein letzter Aspekt: Da Sie den Einsatz lokaler Diabetes-Datenmanagement-Lösungen erwähnen, die aus Gründen der IT-Sicherheit keine Internetverbindung benötigen - dies verkennt, dass Cloud-Dienste ein viel höheres Maß an IT-Sicherheit bieten, als es lokale Lösungen in Praxen oder Krankenhäusern je bieten könnten. Denn Cloud-Dienste enthalten viele fortschrittliche Sicherheitsfunktionen, die garantieren, dass Daten sicher gespeichert und verarbeitet werden. Funktionen wie granulare Berechtigungen und Zugriffsmanagement über Rollenkonzepte können den Zugang zu sensiblen Daten auf die Mitarbeiter beschränken, die ihn benötigen, und so die Angriffsfläche für böswillige Akteure verringern. Cloud-Anbieter wie Dexcom haben für ihre Plattformen und die von ihnen verarbeiteten Daten grundlegende Schutzmechanismen wie Authentifizierung, Zugriffskontrolle und Verschlüsselung implementiert. Das ist mehr, als der typische Gesundheitsversorger (insbesondere in kleineren Praxen) jemals vernünftigerweise umsetzen kann.

\*\*\*



## BVKD-Geschäftsstelle

**Von:** Schneider, Florian <florian.schneider.fs3@roche.com>  
**Gesendet:** Mittwoch, 27. Oktober 2021 18:30  
**An:** BVKD-Geschäftsstelle  
**Cc:** Schneider, Steffen  
**Betreff:** Re: Unsere Anfrage zum Datenschutz - VORAB PER E-MAIL

Sehr geehrter Herr Jannaschk,

wie angekündigt, kommen wir zurück auf Ihre E-Mail vom 4. Oktober 2021 und die darin gestellten Fragen zu unseren Geräten Accu-Chek Insight und Accu-Chek Combo. Gerne beantworten wir Ihre Fragen im Folgenden.

### Zu Frage 1:

Auch ohne Cloud-Lösung lassen sich die Daten Offline, beispielsweise über die Desktop-Lösung Smart Pix Software verarbeiten. Bitte entnehmen Sie der nachfolgenden Tabelle, welche Daten in welchem Anwendungsszenario in welchem Umfang verfügbar sind:

<b>Diabetes Management Systeme (DMS)</b>	<b>Roche: Roche Diabetes Care Plattform (SaaS)</b>	<b>Roche: Smart Pix Software (offline DMS)</b>	<b>Diabeloop: Yourloops (SaaS)</b>	<b>DMS von Drittanbietern</b>
<b>Diabetes Gerät für Patient</b>				
<b>Combo Pumpe</b>	Hochladen aller Daten möglich mittels eines kompatiblen Infrarot-Lesegeräts (360 cable, Realtyme cable, SmartPix Device Reader II) möglich.	Hochladen aller Daten möglich mittels eines kompatiblen Infrarot-Lesegeräts (SmartPix Device Reader I oder II) möglich.	-	DMS von Drittanbietern können über die offene Schnittstelle des Smart Pix Device Reader II nahezu alle Daten auslesen (Insulinsensitivität und Insulin-Kohlenhydrat-Verhältnis werden in der offenen Schnittstelle nicht zur Verfügung gestellt).
<b>Combo Diabetes Manager</b>	Pumpe und Diabetes Manager müssen beide separat ausgelesen werden.	Pumpe und Diabetes Manager müssen beide separat ausgelesen werden.		
<b>Insight Pumpe mit mySugr pump control module</b>	Der Patient kann den Bolus von der mySugr App mit der Gesundheitseinrichtung teilen.	Durch direktes Pairing der Insight Pumpe mit dem Smart Pix Device Reader können die Pumpendaten hochgeladen werden. Manuelle Einträge die in der mySugr App gespeichert sind und über die Reportfunktion als CSV-Datei exportiert werden, können mit einem Plugin für Smart Pix Software hochgeladen werden ( mit Ausnahme der Insulinsensitivität und des Insulin-Kohlenhydrat-Verhältnisses).	-	Sowohl aus der Smart Pix Software als auch aus mySugr können die Daten exportiert werden, die ggf. in DMS von Drittanbietern importiert werden können.

<b>Insight Pumpe (Standalone)</b>	-	Durch direktes Pairing der Insight Pumpe mit dem Smart Pix Device Reader können die Pumpendaten hochgeladen werden. Weitere Daten sind nicht verfügbar.	-	Aus der Smart Pix Software können die Daten exportiert werden, die ggf. in DMS von Drittanbietern importiert werden können.
<b>Insight Pumpe mit Diabeloop System (AID)</b>	-	-	Automatisches Hochladen der Daten von dem Diabetes Manager in die Yourloops Plattform. Patient kann diese Daten dann von dort mit dem HCP teilen.	-
<b>Insight Pumpe mit Diabetes Manager</b> (nur Bestandskunden, weil Diabetes Manager nicht mehr vertrieben wird)	Hochladen aller Daten durch das Auslesen des Diabetes Manager möglich (durch einfache Verbindung des Diabetes Manager mit einem Standard USB-Kabel mit dem Computer)	Hochladen aller Daten durch das Auslesen des Diabetes Manager möglich (durch einfache Verbindung des Diabetes Manager mit einem Standard USB-Kabel mit dem Computer)	-	DMS von Drittanbietern können über die offene Schnittstelle des Smart Pix Device Reader II nahezu alle Daten auslesen (Insulinsensitivität und Insulin-Kohlenhydrat-Verhältnis werden in der offenen Schnittstelle nicht zur Verfügung gestellt)

**Zu Frage 2:**

Die führenden IT-Systeme im Krankenhaus (KIS/LIS) können die Daten jederzeit über die Schnittstelle importieren und so einer weiteren internen, nicht cloud-basierten Verarbeitung zuführen. Hierfür bestehen dann die in der o.g. Tabelle aufgeführten Möglichkeiten.

**Zu Frage 3:**

Mit Ausnahme von offiziellen Partnerschaften, können wir generell keine Aussagen zur Kompatibilität unser Geräte mit Drittanbietern treffen. Der Smart Pix Device Reader II hat eine offene Schnittstelle, der einen Export aller Daten für Lesegeräte ermöglicht, mit Ausnahme der Daten zur Insulinsensitivität und zum Insulin-Kohlenhydrat-Verhältnis. Die Daten werden von Diabetes-Management-Systemen verschiedener Drittanbieter genutzt, allerdings können wir eine Integration und Kompatibilität mit unseren Geräten, mit Ausnahme von Diabeloop für die Insight-Pumpe und Diasend für die Solo-Pumpe, nicht garantieren.

Die Geräte unserer jüngsten Generation von Blutzuckermessgeräten funktionieren auf Basis offener Standards entsprechend der Continua Health Alliance, die es jedem mit entsprechendem technischen Wissen erlaubt, unsere Geräte auszulesen. Aus Sicherheitsgründen wird ein Zugriff für ein direktes Auslesen der Pumpen und Diabetesmanager für die Insight- und Combo-Pumpe für Dritte nicht ermöglicht.

Bitte lassen Sie uns wissen, wenn Sie hierzu noch Rückfragen haben.

Mit freundlichen Grüßen

Steffen Schneider  
- International Product Manager -

Florian Schneider  
- Datenschutzbeauftragter -

Am Mo., 4. Okt. 2021 um 20:45 Uhr schrieb Florian Schneider <[florian.schneider.fs3@roche.com](mailto:florian.schneider.fs3@roche.com)>:  
Sehr geehrter Herr Jannaschk,

vielen Dank für Ihre Vorab-E-Mail und Ihre Rückfragen. Ich werde versuchen, Ihnen möglichst rasch Rückmeldung zu geben.

Freundliche Grüße

Florian Schneider

Am Mo., 4. Okt. 2021 um 19:16 Uhr schrieb BVKD-Geschäftsstelle <[geschaefsstelle@die-diabetes-kliniken.de](mailto:geschaefsstelle@die-diabetes-kliniken.de)>:

Sehr geehrter Herr Schneider,

wir kommen zurück auf unsere Anfrage zum Datenschutz vom 05.03.2021 und bedanken uns zunächst nochmals herzlich für Ihre Rückantwort.

Zwischenzeitlich konnten wir nun alle Stellungnahmen der angeschriebenen Anbieter sichten. Leider müssen wir feststellen, dass die Antworten einiger Hersteller sich nicht mit der unlängst veröffentlichten Rechtsauffassung der deutschen Datenschutzbehörden decken. Manche Ausführungen stimmen auch nicht mit anderslautenden Verlautbarungen in Werbung und Produktunterlagen überein.

Vor diesem Hintergrund beabsichtigen wir, die erhaltenen Antworten einer juristischen Prüfung zuzuführen sowie gegebenenfalls den Datenschutzbehörden vorzulegen, damit wir abschließend unseren Mitgliedern rechtssichere Empfehlungen geben können.

Wir gehen davon aus, dass eine solche Klärung auch in Ihrem Interesse ist. Daher bitten wir um die Beantwortung der nachfolgenden, weiteren Fragen zu jedem Ihrer nachstehenden Hilfsmittel:

### **Accu-Chek Insight, Accu-Chek Combo**

#### **Frage 1:**

Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung,

## BVKD-Geschäftsstelle

---

**Von:** Wernicke, Julia <jwernicke@menarini-berlin.de>  
**Gesendet:** Mittwoch, 13. Oktober 2021 10:15  
**An:** BVKD-Geschäftsstelle  
**Cc:** Kleist, Daniel; Mailbox BC-dpo.germany  
**Betreff:** Re: Unsere Anfrage zum Datenschutz - VORAB PER E-MAIL

**Kennzeichnung:** Zur Nachverfolgung  
**Kennzeichnungsstatus:** Erledigt

Sehr geehrter Herr Jannaschk,

vielen Dank für Ihre erneute Anfrage. Gerne beantworten wir Ihre weiteren Fragen zum rtCGM-System GlucoMen Day CGM, das wir als A. MENARINI DIAGNOSTICS Deutschland - eine Division der Berlin-Chemie AG gegenwärtig vertreiben.

### **Antwort zur Frage 1:**

GlucoMen Day® CGM ist ein System zur kontinuierlichen Glukosemessung. Die Glukosewerte werden in die dazugehörige GlucoMen Day® App über Bluetooth übertragen. Die in der App hinterlegten Daten können ohne Einbindung Dritter in Form eines

1). In-App-Berichts geteilt werden. Für den ausgewählten Analysezeitraum (3, 7, 14 oder 28 Tage) werden die Glukosedaten statistisch ausgewertet (AGP, Glukosedurchschnitt, TiR, Standardabweichung und Variationskoeffizient) und grafisch aufbereitet. Dieser Bericht kann direkt in der App angezeigt und analysiert werden. Darüber hinaus besteht die Möglichkeit erstellte Berichte zu exportieren und bspw. per E-Mail in Form einer PDF-Datei bereitzustellen.

2.) Neben der Aufbereitung der Daten in der App können die Rohdaten der Glukosemessung in Form einer CSV-Datei exportiert und in kompatible, lokale Analyseprogramme (bspw. SmartPix, DIABASS oder SiDiary) importiert werden.

Lediglich **optional** und **nach ausdrücklicher Freigabe** durch den Nutzer können die Daten aus der App in die Cloud des Herstellers WaveForm Technologies Inc./AgaMatrix Inc. gesendet werden. Beachten Sie in diesem Zusammenhang auch unsere Ausführungen vom 25.03.2021.

### **Antwort zur Frage 2:**

Eine Nutzung des rtCGM-System GlucoMen Day CGM ist ohne Verwendung einer Cloud-Verbindung möglich. Beachten Sie hierzu unsere ausführliche Antwort zur Frage 1.

### **Antwort zur Frage 3:**

Die zugrundeliegenden Daten können aus der App heraus mittels CSV-Datei exportiert und ohne Einbindung Dritter in lokal installierte Analyseprogramme wie Smartpix, Diabass oder SiDiary importiert werden. Der Export der CSV-Datei kann ohne verfügbare Internetverbindung per Bluetooth erfolgen, sofern die Klinik über die technische Ausstattung verfügt. Hierbei wird die Datei per Bluetooth-Verbindung vor Ort in der Klinik an den Rechner übertragen auf dem die lokale Analysesoftware installiert ist und in das verwendete Programm importiert.

Darüber hinaus kann die Übertragung der Daten in die offline-basierten Datenmanagement Lösungen per E-Mail erfolgen. Entweder direkt an einen Account der behandelnden Klinik oder an den E-Mail Account des Anwenders, der von dort die Datei mittels eines externen und mobilen Speichermediums in der Klinik bereitstellt. Bei Nutzung von Diabass besteht weiterhin die Möglichkeit der DIABASS SecureSend Funktion per App. Mit DIABASS SecureSend kann der Patient die Daten aus der Offline-Nutzung sicher und ohne Zugriff Dritter an den Arzt/Klinik schicken: der Arzt/Klinik erstellt dem Patienten hierzu auf Knopfdruck ein Infoblatt mit Versanddaten, dazu kann er ihm eine Anleitung mitgeben. Die Daten kommen dann beim Arzt/Klinik direkt per E-Mail in Form eines verschlüsselten Datenpakets an. Diese werden dann nach Wahl des Arztes/Klinik entweder halbautomatisch (d.h. per Doppelklick auf den Mailanhang) oder vollautomatisch (automatischer Abruf der E-Mails) ins DIABASS eingepflegt.

Im Fall von Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen  
Dr. Julia Wernicke - Datenschutzbeauftragte

Daniel Kleist - Leiter Operatives Geschäft

-----  
i.V. Dr. Julia Wernicke  
Data Protection Officer, Head of Data Protection  
Rechtsanwältin (Syndikusrechtsanwältin)

BERLIN-CHEMIE AG/ A. Menarini Research & Business Service GmbH  
Glienicke Weg 125, 12489 Berlin

Tel.: [+49 \(0\)30 / 67 07 33 85](tel:+493067073385)  
Mobil: +49 152 2250 6829  
Fax: [+49 \(0\)30 / 67 07 31 97](tel:+493067073197)  
Email: [jwernicke@menarini-berlin.de](mailto:jwernicke@menarini-berlin.de)  
[www.berlin-chemie.de](http://www.berlin-chemie.de)

Am Mo., 4. Okt. 2021 um 19:16 Uhr schrieb BVKD-Geschäftsstelle <[geschaefsstelle@die-diabetes-kliniken.de](mailto:geschaefsstelle@die-diabetes-kliniken.de)>:

Sehr geehrte Frau Dr. Wernicke,

wir kommen zurück auf unsere Anfrage zum Datenschutz vom 05.03.2021 und bedanken uns zunächst nochmals herzlich für Ihre Rückantwort.

Zwischenzeitlich konnten wir nun alle Stellungnahmen der angeschriebenen Anbieter sichten. Leider müssen wir feststellen, dass die Antworten einiger Hersteller sich nicht mit der unlängst veröffentlichten Rechtsauffassung der deutschen Datenschutzbehörden decken. Manche Ausführungen stimmen auch nicht mit anderslautenden Verlautbarungen in Werbung und Produktunterlagen überein.

Vor diesem Hintergrund beabsichtigen wir, die erhaltenen Antworten einer juristischen Prüfung zuzuführen sowie gegebenenfalls den Datenschutzbehörden vorzulegen, damit wir abschließend unseren Mitgliedern rechtssichere Empfehlungen geben können.

Wir gehen davon aus, dass eine solche Klärung auch in Ihrem Interesse ist. Daher bitten wir um die Beantwortung der nachfolgenden, weiteren Fragen zu jedem Ihrer nachstehenden Hilfsmittel:

## **Glucomen Day**

### **Frage 1:**

Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung,

## BVKD-Geschäftsstelle

---

**Von:** Datenschutz - Ypsomed GmbH <datenschutz@ypsomed.de>  
**Gesendet:** Mittwoch, 17. November 2021 13:43  
**An:** BVKD-Geschäftsstelle  
**Betreff:** AW: Unsere Anfrage zum Datenschutz - VORAB PER E-MAIL

Sehr geehrter Herr Jannaschk,

gerne beantworten wir Ihre Fragen aus dem Schreiben vom 04. Oktober 2021 bezüglich der datenschutzrechtlichen Bedingungen bei der Nutzung unserer mylife Software und entschuldigen uns für die lange Bearbeitungszeit.

### Frage 1:

**Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung, Ereignisse, Alarmer, manuelle Eingaben, Basalratenprogrammierung, ...) für ein computergestütztes Diabetes-Datenmanagement genutzt werden, ohne dass hierzu diese Daten an Dritte übermittelt werden (müssen)?**

**Falls ja: Bitte beschreiben Sie die Möglichkeiten, die der Klinik zu Verfügung stehen. Bitte teilen Sie auch mit, wenn und inwieweit sich nicht alle mit dem Hilfsmittel erhobenen Daten auf diese Weise nutzen lassen.**

Die in den mylife Therapiemanagement Produkten gespeicherten Therapiedaten können auf verschiedene Art angezeigt werden. Mit der mylife Software und Cloud sind folgende Berichte möglich:

- Dashboard: Ansicht für den Import und die Synchronisierung von Gerätedaten und für einen schnellen Überblick über die Entwicklungen und Ergebnisse der Therapie
- Übersicht: Grafische Darstellung der Therapiedaten
- Tagebuch: Chronologische Liste aller Informationen, Notizen sowie Daten
- Standardtag: Für ein 24-Stunden-Blutzuckermuster
- Verteilung: Zur Anzeige des Blutzuckerungsverlaufs während des Tages oder in bestimmten Zeiträumen
- Insulinbericht: Zeigt die Insulinmenge, das Basalraten-Bolus-Verhältnis und die Bolusarten an
- Trendbericht: Zum Vergleich der Therapie innerhalb zweier Zeiträume und zur Identifizierung von Optimierungsmöglichkeiten der Therapie
- Pumpeneinstellungen: Dient der automatischen Speicherung der Pumpeneinstellungen bei jedem Datenimport und dem Vergleich der Pumpeneinstellungen zweier Zeiträume. Einstellungen des Bolusvorschlagsrechners werden ebenfalls separat dargestellt.
- Patientenverzeichnis: Nur in der professionellen Version verfügbar. Für Ärzte zur Erstellung, Anzeige und individuellen Verwaltung von Patientendaten relevant
- Einstellungen: Zur Konfiguration der Software entsprechend Ihren Präferenzen

Diese Berichte kann die Klinik mit der mylife Software und Cloud selbst erzeugen oder die Patienten bringen diese mit der mylife Cloud oder mylife Software erzeugten Berichte im PDF-Format mit (via ihr eigenes Patientenkonto).

Die mylife App bietet im Tagebuch eine chronologische, tabellarische Anzeige der erfassten Therapiedaten. Ebenso ist ein PDF-Export eines Teils der genannten Berichte möglich (Pumpeneinstellungen, Statistiken zu Blutzuckerungsverläufen, Insulinverbrauch und eine Tag-für-Tag Übersicht der relevanten Therapiedaten), der mit der Klinik geteilt werden kann.

### Frage 2:

**Wenn der Patient keine Einwilligung zur Datenverarbeitung gemäß den Nutzungsbedingungen der von Ihnen vorgesehenen Cloudlösung(en) erteilen will oder seine Einwilligung später widerruft: Wie können die mit dem Hilfsmittel erhobenen Daten dann weiterhin - über die bloße Möglichkeit zum Ablesen vom Gerätedisplay hinausgehend - im Rahmen eines computergestützten Datenmanagements von der Klinik zur Behandlung genutzt werden, so dass die fehlende Einwilligung zur Datenverarbeitung nicht zu Nachteilen bezüglich der Therapie- und Behandlungsqualität führen muss?**

Sofern jemals ein mylife Cloud Konto bestand, können die Daten daraus vor Schließen des Kontos im PDF- oder CSV-Format exportiert werden.

Es ist mit Hilfe der mylife Software und des mylife (Bluetooth) Dongle möglich die Daten der mylife YpsoPump offline auszulesen und zu exportieren. Ebenso ist das für eine Vielzahl an Blutzuckermessgeräten möglich. Mit der mylife App erfasste CGM-Daten des Dexcom G6 Systems sind aktuell in der Dexcom CLARITY Cloud einsehbar. Wir planen diese bald ebenfalls in der mylife Cloud anzuzeigen.

### Frage 3:

Im klinischen Behandlungsalltag ist sicherzustellen, dass u.a. die Pflichten aus Art. 5 DSGVO (Datenminimierung, Zweckbindung) eingehalten werden und die Vorgaben aus Art. 23 DSGVO erfüllt sind. Zahlreiche Kliniken unterliegen auch dem Anwendungsbereich des BSI-Gesetzes und müssen jede unnötige Schwächung der klinischen IT-Strukturen vermeiden. Vor diesem Hintergrund bevorzugen manche Kliniken anstelle einer cloudbasierten Lösung den Einsatz marktgängiger lokaler Lösungen zum Diabetes-Datenmanagement, die keine Internetverbindung erfordern und die mit zahlreichen Messgeräten bzw. Insulinpumpen unterschiedlicher Hersteller kompatibel sind.

Mit welchen der offline-basierten Datenmanagement-Lösungen anderer Anbieter können die Daten aus dem Hilfsmittel eingelesen werden?

Therapiedaten aus der mylife YpsoPump und den mylife Blutzuckermessgeräten können mit Hilfe der mylife Software und des mylife (Bluetooth) Dongle bzw. USB-Kabeln offline ausgelesen und exportiert werden.

Ebenso ist ein Auslesen der mylife YpsoPump mit der Software Diabass und SmartPix möglich.

Therapiedaten aus der mylife App können offline, also via PDF Bericht exportiert werden. Eine Online-Synchronisierung zwischen der mylife App und der mylife Cloud sind jedoch für Patienten möglich. Aus der mylife Cloud sind verschiedene Exporte möglich. Mit der mylife App erfasste CGM-Daten des Dexcom G6 Systems sind aktuell in der Dexcom CLARITY Cloud einsehbar. Wir planen diese bald ebenfalls in der mylife Cloud anzuzeigen.

Wir hoffen Ihre Fragen hiermit beantwortet zu haben. Bei weiteren Fragen oder Anregungen können Sie sich gerne bei uns melden. Unseren Kunden-Service erreichen Sie von Montag bis Freitag von 8.00 Uhr bis 17.00 Uhr unter der kostenlosen Service-Hotline 0800 9776633.

Mit freundlichen Grüßen

Guelcan Yilmaz  
Datenschutzkoordinatorin DE/AT

Ypsomed GmbH  
Höchster Strasse 70  
65835 Liederbach  
Deutschland

+4969310197138 (direct)

[guelcan.yilmaz@ypsomed.com](mailto:guelcan.yilmaz@ypsomed.com)  
<https://www.ypsomed.com>

mylife™ – More freedom. More confidence. With mylife™. [www.mylife-diabetescare.com/](http://www.mylife-diabetescare.com/)  
Visit us on [Facebook](#) | [Instagram](#) | [YouTube](#) | [Twitter](#)

---

**Von:** BVKD-Geschäftsstelle [mailto:geschaeftsstelle@die-diabetes-kliniken.de]

**Gesendet:** Montag, 4. Oktober 2021 19:16

**An:** Datenschutz - Ypsomed GmbH <datenschutz@ypsomed.de>

**Betreff:** Unsere Anfrage zum Datenschutz - VORAB PER E-MAIL

Sehr geehrte Frau Glaus,

wir kommen zurück auf unsere Anfrage zum Datenschutz vom 05.03.2021 und bedanken uns zunächst nochmals herzlich für Ihre Rückantwort.

Zwischenzeitlich konnten wir nun alle Stellungnahmen der angeschriebenen Anbieter sichten. Leider müssen wir feststellen, dass die Antworten einiger Hersteller sich nicht mit der unlängst veröffentlichten Rechtsauffassung der deutschen Datenschutzbehörden decken. Manche Ausführungen stimmen auch nicht mit anderslautenden Verlautbarungen in Werbung und Produktunterlagen überein.

Vor diesem Hintergrund beabsichtigen wir, die erhaltenen Antworten einer juristischen Prüfung zuzuführen sowie gegebenenfalls den Datenschutzbehörden vorzulegen, damit wir abschließend unseren Mitgliedern rechtssichere Empfehlungen geben können.

## BVKD-Geschäftsstelle

---

**Von:** Dr. Dominik Greim <d.greim@eyedsec.de>  
**Gesendet:** Montag, 18. Oktober 2021 14:00  
**An:** 'geschaefsstelle@die-diabetes-kliniken.de'  
**Cc:** Richard Laqua; Jürgen Friedrich  
**Betreff:** AW: Unsere Anfrage zum Datenschutz

Sehr geehrter Herr Jannaschk, sehr geehrter Bundesverband klinischer Diabetes-Einrichtungen DIE Diabetes Kliniken e.V.

im Auftrag von Herrn Laqua möchte ich, im Folgenden, gerne Ihre Fragen zu den Produkten **Dana RS & Dana i** des Herstellers SOOIL Developments Co. Ltd., vertrieben durch die IME-DC GmbH, beantworten.

### Frage 1:

Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung, Ereignisse, Alarmer, manuelle Eingaben, Basalratenprogrammierung, ...) für ein computergestütztes Diabetes-Datenmanagement genutzt werden, ohne dass hierzu diese Daten an Dritte übermittelt werden (müssen)?

### Antwort 1:

Wir, die IME-DC, nehmen Datenschutz sehr wichtig, insbesondere in Anbetracht dessen, dass es sich bei den mit Hilfe durch uns vertriebener Produkte verarbeiteten Daten gem. Art. 4 DSGVO um Gesundheitsdaten handelt, für die die besonderen Anforderungen des Art. 9 DSGVO gelten. Daher binden durch uns vertriebene Produkte standardmäßig **keine Cloud-Dienste oder sonstige Dienste Dritter ein**, die Verarbeitung findet **ausschließlich lokal** auf dem Gerät statt.

Die in der Pumpe gespeicherten Daten können darüber hinaus mittels der App AnyDana (bereitgestellt durch den Hersteller SOOIL Developments Co. Ltd.) auf ein Smartphone exportiert werden. Auch die Verarbeitung durch diese App erfolgt **ausschließlich lokal auf dem Gerät** des jeweiligen Nutzers und daher auch in dessen Verantwortung. Diese App unterstützt den Export der gespeicherten Datenbank womit die Daten über folgende Universal-Datenmanagementprogramme weiterverarbeitet werden können:

- Diabass
- SiDiary
- Accu Chek Smartpix Software
- Diasend

Da es sich hierbei um Software von nicht mit uns verbundenen Dritten handelt können wir Ihnen zur Einhaltung der datenschutzrechtlichen Gegebenheiten keine Auskunft geben. Inwiefern die Daten durch die jeweilige Software auch diesen Dritten zugänglich gemacht wird sollte in der jeweiligen Datenschutzerklärung des Herstellers einsehbar sein.

### Frage 1, Teil 2:

Falls ja: Bitte beschreiben Sie die Möglichkeiten, die der Klinik zu Verfügung stehen. Bitte teilen Sie auch mit, wenn und inwieweit sich nicht alle mit dem Hilfsmittel erhobenen Daten auf diese Weise nutzen lassen.

### Antwort 1, Teil 2:

Unseres Wissens nach funktionieren die Programme Diabass, SiDiary Professional & Accu Chek Smartpix Software ohne die Übertragung der Daten an den jeweiligen Softwarehersteller oder etwaige andere Dritte. Hierzu sollte jedoch der jeweiligen Hersteller separat kontaktiert werden, da wir über Produkte anderer Hersteller keine rechtssicheren Auskünfte geben können.

Um die Daten von den Geräten Dana RS & Dana i auslesen zu können wird die App AnyDana (für mobile Endgeräte) benötigt. Diese stellt per Bluetooth eine Verbindung mit den Insulinpumpen her und speichert anschließend die Daten lokal auf dem Endgerät. **Es erfolgt keine Übertragung der Daten an uns oder Dritte, die App hat keinerlei Cloud-Funktion.** Von dort aus können die Daten dann wie oben beschrieben exportiert und mit den o.g. Programmen von Drittherstellern verarbeitet werden. Hinsichtlich der Frage inwieweit sich auf diesem Weg nicht alle erhobenen Daten auf diese Weise nutzen lassen müssen wir sie leider wiederum an den jeweiligen Hersteller verweisen, da uns deren einzelne Produktspezifikationen nicht bekannt sind.



### Frage 2:

Wenn der Patient keine Einwilligung zur Datenverarbeitung gemäß den Nutzungsbedingungen der von Ihnen vorgesehenen Cloudlösung(en) erteilen will oder seine Einwilligung später widerruft: Wie können die mit dem Hilfsmittel erhobenen Daten dann weiterhin - über die bloße Möglichkeit zum Ablesen vom Gerätedisplay hinausgehend – im Rahmen eines computergestützten Datenmanagements von der Klinik zur Behandlung genutzt werden, so dass die fehlende Einwilligung zur Datenverarbeitung nicht zu Nachteilen bezüglich der Therapie- und Behandlungsqualität führen muss?

### Antwort 2:

Wir, die IME-DC GmbH, sowie der Hersteller der genannten Insulinpumpen, die SOOIL Developments Co. Ltd. sehen **keine Cloudlösung** zur Verarbeitung der durch die Pumpen erhobenen Daten vor. Die optional verfügbare App AnyDana zum Auslesen der Daten von den Pumpen speichert ebenso wie die Pumpen selbst Daten **ausschließlich lokal**. Es erfolgt daher grundsätzlich keine Weitergabe von Daten an uns oder Andere und damit auch keine Verarbeitung im Sinne der DSGVO durch uns oder Andere. Daher ist aus unserer Sicht keine Einwilligung zur Datenverarbeitung gem. Art. 9 Abs. 2 lit. a notwendig. Inwiefern die unter Frage 1 genannten Programme von Drittherstellern Daten weitergeben entzieht sich unseres Verantwortungsbereiches und muss daher bei diesen erfragt werden. Sofern die Verarbeitung durch die Software der genannten Dritthersteller ausschließlich lokal (in den Kliniken) erfolgt sehen wir keinerlei Einschränkungen hinsichtlich der Therapie & Behandlungsqualität bei Nicht-Vorliegen einer rechtswirksamen Einwilligung des Patienten.

### Frage 3:

Im klinischen Behandlungsalltag ist sicherzustellen, dass u.a. die Pflichten aus Art. 5 DSGVO (Datenminimierung, Zweckbindung) eingehalten werden und die Vorgaben aus Art. 23 DSGVO erfüllt sind. Zahlreiche Kliniken unterliegen auch dem Anwendungsbereich des BSI-Gesetzes und müssen jede unnötige Schwächung der klinischen IT-Strukturen vermeiden. Vor diesem Hintergrund bevorzugen manche Kliniken anstelle einer cloudbasierten Lösung den Einsatz marktgängiger lokaler Lösungen zum Diabetes-Datenmanagement, die keine Internetverbindung erfordern und die mit zahlreichen Messgeräten bzw. Insulinpumpen unterschiedlicher Hersteller kompatibel sind.

Mit welchen der offline-basierten Datenmanagement-Lösungen anderer Anbieter können die Daten aus dem Hilfsmittel eingelesen werden?

### Antwort 3:

Die genannten Insulinpumpen Dana RS & Dana i sind gem. Art 5 DSGVO auch mit der zugehörigen App AnyDana vollkommen frei von Cloud-Diensten. Nach unserem Verständnis ermöglichen wir so Kliniken alle Anforderungen der DSGVO in Ihrem Betrieb praxisorientiert und pragmatisch umzusetzen. Inwiefern hierbei die Einschränkung der Rechte Betroffener gem. Art. 23 DSGVO zum Tragen kommt ist uns nicht bekannt. Unsere Produkte erfordern lediglich zur Installation der App „AnyDana“ eine aktive Internetverbindung, da diese aus den gängigen App-Stores heruntergeladen werden muss. Dies stellt aus unserer Sicht keine Schwächung der klinischen IT-Infrastruktur dar, sofern entsprechende Richtlinien & Prozesse zur Freigabe von Apps und der Verarbeitung von Daten im Rahmen des mobile device management (z.B. gem. der IT-Sicherheitsrichtlinie der KBV gem. §75b SGB V, Anlagen 1, 2 & 3) umgesetzt werden. Darüber hinausgehende Maßnahmen zum Einsatz unserer Produkte insbesondere in Hinblick auf die Anwendbarkeit des BSIG und der zugehörigen KritisV sind aus unserer Sicht nicht notwendig.

Hinsichtlich der Funktionalität der Produkte von Drittherstellern können wir grundsätzlich keine rechtssichere Auskunft geben. Die jeweiligen Hersteller sollten daher separat hinsichtlich Ihrer Anforderungen kontaktiert werden.

Nach unserem Wissen arbeiten folgende Programme von Drittherstellern ausschließlich lokal:

Diabass

<https://www.diabass.com/de#funktionen>

SiDiary Professional

<https://www.sidiary.de/sidiary-professional-2395.asp?activeBanner=8>

Accu Chek Smartpix Software

<https://www.accu-chek.de/produkte/datenmanagement/smart-pix-software/overview>

Ich hoffe ich konnte weiterhelfen, falls weitere Fragen bestehen stehe ich jederzeit zur Verfügung.

mit freundlichen Grüßen

**Dr. Dominik Greim**

Datenschutz & IT-Sicherheitsberater

EMAIL [d.greim@eyedsec.de](mailto:d.greim@eyedsec.de)

MOBIL +49 151 448 266 65

EYEDSEC - INFORMATION SECURITY GMBH

Friedrichstr. 25 / 95444 Bayreuth

Internet: [www.eyedsec.de](http://www.eyedsec.de)

Tel: 0921 23059936

Fax: 0921 15082070

eyeDsec - Information Security GmbH/ Geschäftsleitung: Matthias Mühlhaus, Richard Laqua/ Sitz in Bayreuth/ Amtsgericht Bayreuth/ HRB 5841

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Mail ist nicht gestattet. This e-mail may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

---

**Von:** BVKD-Geschäftsstelle <[geschaeftsstelle@die-diabetes-kliniken.de](mailto:geschaeftsstelle@die-diabetes-kliniken.de)>

**Gesendet:** Montag, 4. Oktober 2021 19:16

**An:** Datenschutz <[datenschutz@eyedsec.de](mailto:datenschutz@eyedsec.de)>

**Betreff:** Unsere Anfrage zum Datenschutz - VORAB PER E-MAIL

Sehr geehrter Herr Laqua,

wir kommen zurück auf unsere Anfrage zum Datenschutz vom 05.03.2021 und bedanken uns zunächst nochmals herzlich für Ihre Rückantwort.

Zwischenzeitlich konnten wir nun alle Stellungnahmen der angeschriebenen Anbieter sichten. Leider müssen wir feststellen, dass die Antworten einiger Hersteller sich nicht mit der unlängst veröffentlichten Rechtsauffassung der deutschen Datenschutzbehörden decken. Manche Ausführungen stimmen auch nicht mit anderslautenden Verlautbarungen in Werbung und Produktunterlagen überein.

Vor diesem Hintergrund beabsichtigen wir, die erhaltenen Antworten einer juristischen Prüfung zuzuführen sowie gegebenenfalls den Datenschutzbehörden vorzulegen, damit wir abschließend unseren Mitgliedern rechtssichere Empfehlungen geben können.

Wir gehen davon aus, dass eine solche Klärung auch in Ihrem Interesse ist. Daher bitten wir um die Beantwortung der nachfolgenden, weiteren Fragen zu jedem Ihrer nachstehenden Hilfsmittel:

**Dana RS, Dana i**

**Frage 1:**

Die ledigliche Möglichkeit zum Ablesen des Gerätedisplays ist für eine CSII- bzw. rtCGM-Therapie regelmäßig nicht ausreichend. Können die mit dem Hilfsmittel erhobenen Rohdaten (z.B. Glukosewerte, Insulinausschüttung, Ereignisse, Alarmer, manuelle Eingaben, Basalratenprogrammierung, ...) für ein computergestütztes Diabetes-Datenmanagement genutzt werden, ohne dass hierzu diese Daten an Dritte übermittelt werden (müssen)?

Falls ja: Bitte beschreiben Sie die Möglichkeiten, die der Klinik zu Verfügung stehen. Bitte teilen Sie auch mit, wenn und inwieweit sich nicht alle mit dem Hilfsmittel erhobenen Daten auf diese Weise nutzen lassen.

**Frage 2:**

Wenn der Patient keine Einwilligung zur Datenverarbeitung gemäß den Nutzungsbedingungen der von Ihnen vorgesehenen Cloudlösung(en) erteilen will oder seine Einwilligung später widerruft: Wie können die mit dem Hilfsmittel erhobenen Daten dann weiterhin - über die bloße Möglichkeit zum Ablesen vom Gerätedisplay hinausgehend - im Rahmen eines computergestützten Datenmanagements von der Klinik zur Behandlung genutzt werden, so dass die fehlende Einwilligung zur Datenverarbeitung nicht zu Nachteilen bezüglich der Therapie- und Behandlungsqualität führen muss?