**Datenschutzkonzept der Myosotis GmbH für die Kommunikationsplattform myo (Stand 09.04.2020)**

Datensicherheit und Datenschutz haben höchste Priorität. Wir erfüllen nicht nur die gesetzlichen Bestimmungen, sondern sind mit der ISO 27001 vom TÜV Süd geprüft und sind mit dem ePrivacy Seal EU Siegel zertifiziert. Dieses Dokument enthält Details unserer Datenschutz- und Sicherheitsverfahren und -systeme.

## 1 Datenschutzrechtliche Struktur

Wir betreiben unsere Apps und die dazugehörige Infrastruktur als Auftragsverarbeiter für die teilnehmenden Einrichtungen. Dies umfasst die Speicherung sämtlicher Kontaktdaten von Bewohnern, Angehörigen und Mitarbeitern sowie alle Inhaltsdaten. Die Kontrolle über diese Daten liegt ausschließlich bei den Einrichtungen, unseren Kunden, und wir verarbeiten sie streng weisungsgebunden. Hierzu verpflichten wir uns jeder Einrichtung gegenüber in einer den Anforderungen des Art. 28 DSGVO entsprechenden Auftragsverarbeitungsvereinbarung. Selbstverständlich verpflichtet sich Myosotis darin zur Einhaltung angemessener technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

Darüber hinaus erheben und verarbeiten wir einige Daten auch in eigener Verantwortlichkeit unabhängig von den teilnehmenden Einrichtungen. Dies betrifft folgende Daten und Vorgänge:

- Kontaktdaten von Ansprechpartnern bei teilnehmenden Einrichtungen, die zur Vertragsabwicklung benötigt werden
- E-Mails, Schriftverkehr und sonstige Anfragen, die direkt an Myosotis gerichtet werden
- Statistiken, die von den App Stores (Google Play und Apple AppStore) automatisch allen Anbietern von Apps zur Verfügung gestellt werden
- Statistiken, die wir innerhalb von unseren Apps auf nicht-personenbezogener Basis erheben
- Daten zu Fehlermeldungen innerhalb unserer Apps. Diese Daten sind in aller Regel anonym, können in Einzelfällen aber auch pseudonyme Daten über Endgeräte enthalten

Über die Erhebung und Verarbeitung dieser Daten in eigener Verantwortung weisen wir in einer der Datenschutzerklärung hin.

## 2 Freiwillige Zertifizierungen

Wir werden kontinuierlich von externen Firmen geprüft und haben folgende Informationssicherheits-Zertifizierungen:

- ISO / IEC 27001
- ePrivacy Seal EU

## 3 Weitere Information zur unserer Kommunikationsplattform

### 3.1 Hosting der Kommunikationsplattform

Für unsere Cloud-Infrastruktur benutzen wir den Anbieter Amazon Web Services EMEA SARL, Luxemburg (AWS Europe“) mit Serverstandort in Frankfurt am Main, Deutschland.

AWS bietet state-of-the-art Sicherheitsstandards, insbesondere:

- Verschlüsselung aller Datenträger
- AWS Europe verpflichtet sich jeder Zeit jede Maßnahme zu ergreifen, die den Schutz vertraulicher, persönlicher und personenbezogener Daten gewährleistet.
- AWS Europe schützt wir alle Server und Datenspeicher vor unbefugtem, physischen Zugriff mit allen verfügbaren Mitteln
- AWS Europe überwacht alle Dienste mit höchstmöglicher Verfügbarkeit und höchstmöglicher Sicherheit
- ISO 27001-zertifizierte Rechenzentren (https://aws.amazon.com/de/compliance/iso-27001-faqs/)
- Zertifizierung nach ISO 27018 (Security Techniques – Cloud (https://aws.amazon.com/de/compliance/iso-27018-faqs/)

Die Myosotis GmbH hat nach sorgfältiger Prüfung und Begutachtung des Marktes in Zusammenarbeit mit seinen Anwälten, Beratern und Zertifizierer AWS als bevorzugten Cloud Service Provider befunden. Wir haben mit AWS Europa einen Auftragsverarbeitungsvertrag abgeschlossen, der den Vorrausetzungen des Art. 28 DSGVO entspricht.

Mehr Informationen darüber erhalten Sie hier:

- https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf
- https://aws.amazon.com/de/compliance/gdpr-center/

### 3.2 Speicherung auf mobilen Endgeräten

Wir bieten Anwendungen für die Android und iOS Plattformen an. Beide Systeme schotten unsere Anwendungen von weiteren Anwendungen des Nutzers ab. Die gespeicherten Daten werden auf den Geräten verschlüsselt abgelegt.

### 3.3 Transportverschlüsselung

Sämtliche Kommunikation zwischen den Web-Backends, Web-Frontends und unserer mobilen Anwendungen finden verschlüsselt statt. Entsprechend der Richtlinie zur Klassifizierung von Informationen, sowie rechtlicher und vertraglicher Anforderungen, muss die Organisation individuelle Systeme oder Informationen durch den Einsatz der folgenden Verschlüsselungskontrollen schützen:

### 3.4 Passwords

| System | Algo-rithm | Strength | Notes |
|---|---|---|---|
| Myo Backend | bcrypt | Random salt generated internally, 10 log rounds | Confirmed |
| Myo Auth | bcrypt | Random salt generated internally, 10 log rounds | Confirmed |

### 3.5 HTTPS

| System | Algorithm | Notes |
|---|---|---|

| | | |
|---|---|---|
| Myo Backend | TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256 | Confirmed |
| Myo Auth | TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256 | Confirmed |
| Myo AASA | TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256 | Confirmed |

### 3.6 Kryptografische Schlüssel

Unser interner Sicherheitsbeauftragter (ISB) ist für die Vorgabe der folgenden Regeln zur Schlüsselverwaltung verantwortlich:

- Generierung privater und öffentlicher kryptografischer Schlüssel
- Aktivierung und Verteilung kryptografischer Schlüssel
- Vorgaben zu Begrenzungen der Gültigkeitsdauer von Schlüsseln und zu ihrem regelmäßigen Austausch (entsprechend der Risikoeinschätzung)
- Archivierung von inaktiven Schlüsseln, die für verschlüsselte elektronische Archive benötigt werden
- Vernichtung von Schlüsseln

Schlüssel werden von ihren Eigentümern entsprechend der oben genannten Regeln verwaltet. Für Schlüssel im Bereich Softwareentwicklung ist der Head of Engineering und Tech Lead zuständig. Kryptografische Schlüssel werden durch den ISB angemessen geschützt. Im Falle von Verlust, Verfälschung oder Zerstörung werden Schlüssel durch den ISB wiederhergestellt.

Unsere Postgres RDS-Client-Instanzen werden mit AES-256-GCM-Schlüsseln verschlüsselt, die im AWS Key Management Service gespeichert sind. Außerdem sind alle Postgres RDS-Instanzen nicht öffentlich zugänglich, sondern nur über ein privates VPN AWS Netzwerk durch Kubernetes.

Unsere AWS S3-Buckets, in denen wir die Benutzer-Mediendateien speichern, werden mit der Server-Side Encryption mit Amazon S3-Managed Keys, AES-256, verschlüsselt. S3 Bucket ist nicht öffentlich zugänglich.

### 3.7 Interne Prozesse

| System | Tool / Algorithmus |
|---|---|
| Festplattenverschlüsselung | Filevault (Mac), Bitlocker (Windows) |
| Zwei-Faktor-Authentifizierung | Authenticator App |
| Mobile Device Management | Google Admin Console |
| Netzwerkverschlüsselung | WPA2 |

### 3.8 Statistiken und Fehleranalyse

Um unsere Apps stetig weiterzuentwickeln und den Bedürfnissen der Anwender begegnen sowie Fehler beheben zu können, verwenden wir für die pseudonyme Analyse der Nutzung unserer App sowie für die pseudonyme Protokollierung von Fehlern Google Firebase, einen Dienst der Google Ireland Limited.

Wir haben mit der Google Ireland Limited eine Auftragsverarbeitungsvereinbarung geschlossen und stellen sicher, die Dienste so datensparsam wie möglich einzusetzen. Insbesondere übermitteln wir keine personenbezogenen Daten wie Namen oder Inhaltsdaten an Google.

Die Nutzung dieser Dienste erfolgt durch Myosotis in eigener datenschutzrechtlicher Verantwortlichkeit und nicht im Auftrag der Einrichtungen. Wir weisen auf die Nutzung der Dienste hin.

## 4 Mitarbeiter

Unsere Mitarbeiter werden auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet (ehemals Datengeheimnis), sind verpflichtet eine Vertraulichkeitserklärung zu unterschreiben und werden regelmäßig im Datenschutz geschult.

## 5 Datenschutzbeauftragter

Als Datenschutzbeauftragten haben wir die OC Services GmbH, Kaiser-Wilhelm-Ring 27-29, 50672 Köln benannt. Zentraler Ansprechpartner ist Diplom-Informationsjurist Michael Schidler (TÜV zertifizierter Datenschutzbeauftragter) Unser Datenschutzbeauftragter ist unter Datenschutzbeauftragter@myo.de zu erreichen.

## 6 Verantwortliche Personen

Das Thema Datensicherheit ist bei Myosotis auf verschiedene Schultern verteilt, um eine fortlaufende Selbstkontrolle zu gewährleisten:

- Als ISB ist unser Mitarbeiterin Cecilia von Oldershausen (Business Managerin) benannt.
- Unser Mitarbeiter Damir Palinic (Head of Engineering und Tech Lead und stellvertretender ISB) ist verantwortlich für die Prüfung und Weiterentwicklung unserer technischen und organisatorischen Maßnahmen.
- Außerdem werden wir von einem Lead Auditor ISO 27001 als externer Berater unterstützt.