**Keyed GmbH** | Datenschutz. Einfach. Sicher.
Siemensstraße 12, DE 48341 Altenberge

**SUSTAYN GmbH**

WorkInn, Lindenallee 41

45127 Essen

## Bestätigung über Einhaltung der technischen und organisatorischen Maßnahmen

Sehr geehrte Damen und Herren,

hiermit bestätigt die Keyed GmbH, insbesondere die zuständigen Datenschutzberater:

1. Herr Nils Möllers
2. Herr Dennis Dase, LL.B.

die Einhaltung der technischen und organisatorischen Maßnahmen i.S.d. des Art. 32 DSGVO bei der SUSTAYN GmbH durch die Begutachtung am 20.08.2021. Die fortlaufende datenschutzrechtliche Optimierung wird in Zusammenarbeit mit der Keyed GmbH erarbeitet.

Mit freundlichen Grüßen

Nils Möllers

**Anlagen:**

1. Technische und organisatorische Maßnahmen
2. ISO27001 Zertifizierung des Rechenzentrums

## 1. Anlage:

## Technische und organisatorische Maßnahmen

Mit diesem Dokument informieren wir Sie über die getroffenen Maßnahmen, welche im Zusammenhang mit Verarbeitungen von personenbezogenen Daten getätigt werden.

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (Art. 32 (1) DSGVO).

| | |
|---|---|
| **Verantwortlicher:** | SUSTAYN GmbH |
| **Anschrift:** | WorkInn, Lindenallee 41<br>45127 Essen |
| **Datenschutz-Team:** | Nils Möllers (Keyed)<br>Dennis Dase (Keyed) |
| **IT-Verantwortlicher:** | Janik Seitzer (SUSTAYN) |
| **Datum:** | 23.08.2021 |

### Grundlegende Angaben

- Es liegt keine Pflicht zur Bestellung eines Datenschutzbeauftragten vor, dennoch wird durch externe Unterstützung ein angemessenes Schutzniveau i.S.d. Art. 32 DSGVO erarbeitet.
- Die Beschäftigten sind auf die Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) verpflichtet.
- Beschäftigte werden regelmäßig zum Schutz personenbezogener Daten unterwiesen.
- Es besteht ein aktuelles Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).

---

**Hinweis**:

Bitte beachten Sie, dass Sie die Angaben wahrheitsgetreu beantwortet worden sind, damit eine grundsätzliche Bewertung des Sicherheitsniveaus vollzogen werden kann. Sofern Aktualisierungen dieser technischen und organisatorischen Maßnahmen stattfinden, ist der Auftragsverarbeiter gem. Art. 28 Abs. 2 DSGVO verpflichtet dem Verantwortlichen eine Information diesbezüglich zukommen zu lassen oder sogar eine schriftliche Genehmigung einzuholen.

Grundsätzlich gilt unter Maßgabe des Art. 32 Abs. 1 DSGVO: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“, daher werden im Folgenden die Maßnahmen zur Sicherheit der Verarbeitungen aufgelistet. Beachten Sie bitte hierbei, dass sich gewisse Maßnahmen auf das Rechenzentrum der SUSTAYN GmbH (AWS) beschränken und wiederum andere Maßnahmen sich auf die Arbeitsplätze der SUSTAYN GmbH beziehen. Wir machen Ihnen jeweils bei den Maßnahmen erkenntlich, worauf sich eine konkrete Maßnahme bezieht, sollte es sich jeweils nur auf eine Ebene beziehen.

# Technische und organisatorische Maßnahmen im Detail

## 1. Maßnahmen zur Gewährleistung der Vertraulichkeit

### 1.1 Zutrittskontrolle (Räumlicher Zutrittsschutz)

Sicherheitsmaßnahmen des Rechenzentrums:

- Einsatz von Berechtigungsausweisen.
- Einsatz von elektronischen Zutrittscodekarten/ Zutrittstransponder.
- Bestehen eines Zutrittsberechtigungskonzeptes.
- Einsatz einer Videoüberwachung zum Zweck der Zutrittskontrolle.
- Einsatz einer Alarmanlage.
- Es besteht ein Schlüsselkonzept.
- Einsatz von Besucherausweisen.
- Begleitung von Besucherzutritten durch eigene Mitarbeiter oder Sicherheitspersonal.
- Sicherung auch außerhalb der Arbeitszeit durch Werkschutz.

### 1.2 Zugangskontrolle (Ein unbefugter Zugang und die Nutzung Unbefugter von IT-Systemen ist zu verhindern.)

Sicherheitsmaßnahmen der Organisation:

- Einsatz geeigneter Verschlüsselung der Netzwerke.
- Passwortsicherung von Bildschirmarbeitsplätzen.
- Verwendung von individuellen Passwörtern bzw. Verhinderung von Gruppen-Passwörtern.
- Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner).
- Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern.
- Einsatz einer Passwort-Richtlinie, welche eine sichere Passwortkomplexität (8 Zeichen, Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern) fordert.
- Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern.
- Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern.
- Prozess zum Rechteentzug bei Austritt von Mitarbeitern.

### 1.3 Zugriffskontrolle (Unerlaubte Tätigkeiten in IT-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.)

Sicherheitsmaßnahmen des Rechenzentrums / Software:

- Festlegung der Zugriffsberechtigung, Einsatz eines Berechtigungskonzeptes, sowie Sichere Verwaltung des Zugriffs auf Services und Ressourcen (AWS IAM).
- Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung.
- Regelmäßige Überprüfung von Berechtigungen.
- Protokollierung von Dateizugriffen.
- Protokollierung von Dateilöschungen.
- Protokollierung von Dateiveränderungen.
- Einsatz einer Firewall inkl. Spam-Schutz, sowie DDoS-Schutz (AWS Shield).
- Einsatz von Verschlüsselungsmechanismen (AWS Macie).

Sicherheitsmaßnahmen der Organisation:

- Einsatz einer Anti-Viren-Schutz Lösung auf jedem Endgerät.
- Verschlüsselung der Speichermedien eines Endgerätes.

Alle Daten, die über das AWS Global Network fließen, das unsere Rechenzentren und Regionen verbindet, werden automatisch auf der physischen Ebene verschlüsselt, bevor sie unsere abgesicherten Standorte verlassen. Es gibt noch weitere Verschlüsselungsebenen wie zum Beispiel für den gesamten regionsübergreifenden VPC Peering Traffic und Customer- oder Service-to-Service TLS-Verbindungen.

**1.4 Auftragskontrolle (Es ist sicherzustellen, dass Dienstleister, welche im Auftrag Daten verarbeiten, nur gemäß der Weisung des Auftraggebers Daten verarbeiten.)**

Sicherheitsmaßnahmen der Organisation:

- Vertragsgestaltung der Auftragsverarbeitung gem. gesetzlichen Vorgaben (Art. 28 DSGVO).
- Einschlägige Verarbeitungen finden erst nach Abschluss der Auftragsverarbeitung statt.
- Zentrale Erfassung vorhandener Dienstleister und Auftragsverarbeiter im Datenschutz-Management-System.
- Es werden Kontrollen der technischen und organisatorischen Maßnahmen vor Verarbeitungsbeginn durchgeführt.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen unserer Auftraggeber (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

**1.5 Trennungskontrolle (Es ist sicherzustellen, dass Daten, die zu unterschiedlichen Zwecken, Personen und Unternehmen erhoben wurden, getrennt voneinander verarbeitet werden können.)**

Sicherheitsmaßnahmen des Rechenzentrums / Software:

- Trennung von Kunden (Mandantenfähigkeit der verwendeten Systeme).
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern) in Datenbanken.
- Berechtigungskonzept, das der getrennten Verarbeitung der Daten des Verantwortlichen von Daten anderer Kunden Rechnung trägt.
- Trennung von Entwicklungs-, Test- und Produktivsystemen.

**1.6 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

Sicherheitsmaßnahmen des Rechenzentrums / Software:

- Vor Registrierung werden die Betroffenen über die Nutzungsbedingungen- und Datenschutzerklärungen aufgeklärt und die Einwilligungen eingeholt.

- Die Benutzerdaten werden in einem separaten Dienst (Cognito) und einer separaten Datenbank Tabelle (Dynamodb „profile“) gespeichert. In der übrigen Anwendung wird nur anhand einer „id“ auf das Profil verwiesen, so dass eine Löschung oder Änderung von personenbezogenen Daten problemlos möglich ist, da dies an nur zwei Stellen geschehen muss.
- Das Profil eines Benutzers kann bei einer Anfrage problemlos im JSON Format exportiert und überreicht werden i.S.d. Art. 20 DSGVO.
- Benutzer können selbstständig über die Anwendung die Löschung des eigene Profils beantragen i.S.d. Art. 17 DSGVO.

**2. Maßnahmen zur Gewährleistung der Integrität**

**2.1 Weitergabekontrolle (Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: elektronische Übertragung, Datentransport, sowie deren Kontrolle.)**

Sicherheitsmaßnahmen der Organisation:

- Es besteht eine sichere Versendungsart der Daten zwischen Auftraggeber, Auftragnehmer und Dritten.
- Für den E-Mail Versand sind verschlüsselte ZIP-Dateien möglich.
- Einsatz von VPN-Verbindungen.
- Upload und Download nur über einen SFTP-Server.
- Es findet ein Datenaustausch über eine SSL (https)-Verschlüsselung statt.
- Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle.
- Sicherstellung der Datenträgerentsorgung / Sichere Löschung von Datenträgern.
- Einsatz von Aktenvernichtern (Shredder gem. DIN 66399).
- Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege.

**2.2 Eingabekontrolle (Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.)**

Sicherheitsmaßnahmen des Rechenzentrums / Software:

- Kennzeichnung erfasster Daten.
- Protokollierung von Eingaben/Löschungen.
- Einsatz eines Protokollauswertungssystems.

Sicherheitsmaßnahmen der Organisation:

- Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke.

**3. Maßnahmen zur Gewährleistung der Verfügbarkeit**

**3.1 Verfügbarkeitskontrolle (Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.)**

Sicherheitsmaßnahmen des Rechenzentrums / Software:

- Es bestehen Datensicherungs- und Backupkonzepte.
- Regelmäßige Durchführung der Datensicherungs- und Backupkonzepte.
- Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal.
- Brandmeldeanlagen in Serverräumlichkeiten oder im Rechenzentrum.

- Rauchmelder in Serverräumlichkeiten oder im Rechenzentrum.
- Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten oder im Rechenzentrum.
- Klimatisierte Serverräumlichkeiten.
- Blitz-/ Überspannungsschutz.
- Serverräumlichkeiten in separaten Brandabschnitt.
- Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt.
- Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben).
- USV-Anlage (Unterbrechungsfreie Stromversorgung).
- Einsatz eines Stromgenerators bei Stromausfällen.

Unser Rechenzentrum (AWS) bietet die höchste Netzwerkverfügbarkeit. Jede Serverumgebung in Frankfurt ist vollständig isoliert und besteht aus mehreren AZs, die vollständig isolierte Partitionen der AWS-Infrastruktur sind. Die AWS-Steuerebene und die AWS-Managementkonsole sind zudem über Regionen verteilt und umfassen regionale API-Endpunkte, die so ausgelegt sind, dass sie mindestens 24 Stunden lang sicher funktionieren, wenn sie von den Funktionen der globalen Steuerebene isoliert sind, ohne dass Kunden während einer Isolierung über externe Netzwerke auf die Region oder ihre API-Endpunkte zugreifen müssen.

**4. Maßnahmen zur Gewährleistung der Belastbarkeit**

**4.1 Widerstandsfähigkeit- und Ausfallsicherheitskontrolle**

- Es sind Ausweich-Rechenzentren / Server vorhanden.
- Redundante Datenanbindung.
- Datenspeicherung auf RAID-Systemen (RAID 1 und höher).
- Durchführung von Penetrationstests.
- Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.
- Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.).
- Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.
- Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.

AWS hat international anerkannte Zertifizierungen und Akkreditierungen für die Einhaltung von Datenschutz-Frameworks erhalten, z. B. **ISO 27017** für Cloud-Sicherheit und **ISO 27018** für Cloud-Datenschutz.

**5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

**5.1 Kontrollverfahren**

- Meldung neuer/veränderter Datenverarbeitungsverfahren an das Datenschutz-Team
- Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert.
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen.
- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.

Unser Rechenzentrum identifiziert Bedrohungen durch kontinuierliche Überwachung der Netzwerkaktivität, der Datenzugriffsmuster und des Kontoverhaltens innerhalb der AWS-Umgebung.

## 2. Anlage

### Zertifizierung Amazon Web Services in Frankfurt

Zusätzlicher Hinweis: SUSTAYN trifft bereits geeignete Garantien gem. Art. 46 Abs. 2 lit. c) DSGVO mit zusätzlichen Maßnahmen in Form der Verschlüsselung.


iso_27001_global_certification_aws.pdf

**Kontakt:**
T +49 2505 639797
F +49 2505 639777
E info@keyed.de
W www.keyed.de

**Geschäftsführer:**
Nils Möllers

**Sitz der Gesellschaft:**
Amtsgericht Steinfurt | HRB 11598
Ust-Id.Nr. DE 312621690
Steuer-Nr. 311/5851/3919

**Bankverbindung:**
Volksbank Münsterland Nord eG
IBAN: DE50 4036 1906 7863 6068 00
BIC: GENODEM1IBB