

## ENIT SaaS Leistungen

### 1. Betreiber

Die Enit Energy IT Systems GmbH (ENIT), als verbundenes Konzernunternehmen der proALPHA, betreibt die für die vertragsgegenständlichen Dienstleistungen relevanten Applikationen.

### 2. Rechenzentrum, Verfügbarkeit

- 2.1. Die für die vertragsgegenständlichen Dienstleistungen relevanten Applikationen sind in der AWS-Cloud gehostet, welche im Rechenzentrum von Amazon Web Services, Inc. (kurz „AWS“) in Frankfurt am Main, Deutschland betrieben wird.
- 2.2. Alle vom Rechenzentrum angemieteten Datenräume sind als separate IT-Sicherheitsräume im Sinne des IT-Grundschutzkataloges, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), gemäß Anforderung der Kategorie „Grundschutz“ ausgerüstet. Es wurden spezielle Maßnahmen für Brandschutz, Klimatisierung sowie Überwachung (Zutrittssicherung, Videoüberwachung) getroffen. Die Umgebungsbedingungen wie Temperaturen und Luftfeuchtigkeit werden ständig überwacht, erfasst und aufgezeichnet. Beim Über- oder Unterschreiten von Grenzwerten werden entsprechende Maßnahmen eingeleitet. Die Netzversorgung sowie die Netzersatzanlage (NEA) sowie USV-Anlage erfolgt für das Rechenzentrum mit gesondert bereitgestellter Trafostation des Energieversorgers. Das Rechenzentrum ist über mehrere 10Gbit Leitungen an unterschiedliche Provider angebunden, um ausreichende Bandbreite und Redundanz sicherzustellen.
- 2.3. Die ENIT-Anwendung und Datenbank steht rund um die Uhr – ausgenommen vorher bekannt gemachter Wartungsfenster - zur Nutzung zur Verfügung. Das Rechenzentrum sichert eine durchschnittliche Verfügbarkeit von mindestens 95 % zu.

### 3. SaaS-Dienst / Cloud Server

- 3.1. Der SaaS-Dienst von ENIT bietet ein Mietmodell für die Applikationssoftware ENIT agent und ENIT hub.
- 3.2. Hierfür setzt ENIT Cloud-Infrastruktur ein, die die Hardware, das Betriebssystem, die Netzanbindung und verschiedene Dienstleistungen wie Datensicherung umfassen. Bei der Cloud-Infrastruktur handelt es sich um AWS Lambda serverlose Anwendungen, die durch AWS betrieben werden. Der Leistungsumfang umfasst die Wartung von Servern und Betriebssystemen, die Bereitstellung von Kapazitäten und die automatische Skalierung, die Bereitstellung von Code und Sicherheitspatches.

### 4. Datensicherung

Zur Datensicherung der Cloud-Server wird ein Datensicherungsverfahren verwendet, bei dem der gesamte Server als Image gesichert wird. Es wird dazu keine Netzwerkverbindung zwischen dem Datensicherungssystem und dem Cloud-Server oder administrativen Accounts in den zu sichernden Cloud-Servern benötigt. Dadurch kann eine hohe Sicherheit bei der Durchführung der Datensicherung gewährleistet werden. Die Datensicherungen erfolgen über eine Point-in-Time-Recovery. Die Wiederherstellung wird nach Aufwand berechnet. Die Datensicherungen werden vierzehn (14) Tage vorgehalten.

## 5. Monitoring

Die Cloud-Server werden durch Serverless Infrastruktur (AWS) überwacht. Überwacht werden dabei die Ressourcen (CPU, RAM, Netzwerk, Disk) sowie die für den Betrieb der Server notwendige Infrastruktur.

## 6. Support

Der Support umfasst telefonische Unterstützung während der Servicezeit (üblicherweise Mo - Fr, 08:00 Uhr – 17:00 Uhr). Gesetzliche Feiertage in Baden-Württemberg, der 24.12. bis 31.12. sowie vorher bekannt gemachte Wartungsfenster sind von der Servicezeit ausgenommen.

## 7. Wartungsfenster

Wartungsfenster finden außerhalb der regulären Servicezeiten nach Vorankündigung statt. Bei wichtigen Gründen kann ein Wartungsfenster auch kurzfristig zu jeder Zeit angekündigt und durchgeführt werden. ENIT ist in diesen Wartungsfenstern berechtigt, Anwendungen zu pflegen und / oder Server zu warten, Datensicherungen oder sonstige Arbeiten vorzunehmen. Während solcher Wartungsfenstern kann es zu Nichtverfügbarkeit oder Leistungsreduzierung kommen.

## 8. Firewall

- 8.1. Die ein- und ausgehenden Web-Verbindungen werden mittels modernstem Identity Access Management (IAM), HTTPS-Verbindungen und Auth0 überprüft, überwacht und ggf. abgelehnt und protokolliert.
- 8.2. Bei den Feldgeräten erfolgt mittels VPN-Verbindung (Site-to-Site) eine Authentifizierung an der Core-Firewall und die Verbindung zum Zielsever / Zielnetzwerk.

## 9. Voraussetzungen, die der Kunde sicherstellen muss.

- 9.1. Die Bereitstellung einer angemessenen (Bandbreite, Latenz, Redundanz) Internet-Anbindung auf Kundenseite fällt in den Aufgabenbereich des Kunden.
- 9.2. Die Nutzung des SaaS Dienstes setzen einen aktuellen und von ENIT freigegebenen Browser auf Kundenseite voraus.