Leistungsbeschreibung und Service Level Agreement (SLA)
tisoware SaaS Leistungen

1. Betreiber

1.1. Die tisoware – Gesellschaft für Zeitwirtschaft mbH, Reutlingen, als verbundenes Konzernunternehmen der proALPHA, betreibt die für die vertragsgegenständlichen Dienstleistungen relevanten Applikationen.

2. Rechenzentrum, Verfügbarkeit

2.1. 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.

2.2. Die tisoware Anwendung und Datenbank steht rund um die Uhr – ausgenommen vorher bekannt gemachter Wartungsfenster - zur Nutzung zur Verfügung. Das Rechenzentrum sichert eine durchschnittliche Verfügbarkeit von 99 % zu.

3. SaaS-Dienst / Cloud Server

3.1. Der SaaS-Dienst von tisoware bietet ein Mietmodell für die Applikationssoftware tisoware**.**

3.2. Hierfür setzt tisoware Cloud-Server ein, die die Hardware, das Betriebssystem, die Netzanbindung und verschiedene Dienstleistungen wie Datensicherung umfassen. Bei den Cloud-Servern handelt es sich um virtuelle Server auf der Basis von VMware vSphere in einer aktuellen Version, die auf VMware HA / DRS Clustern betrieben werden und sind somit durch die VMware Hochverfügbarkeitsfunktionen für den Ausfall einer Server Hardware geschützt. Durch ein vollautomatisches Load Balancing werden Cloud-Server entsprechend ihrer Leistungsanforderungen und dynamisch auf unterschiedlicher Hardware verteilt**.**

4. Datensicherung

4.1. Zur Datensicherung der Cloud-Server wird ein Datensicherungsverfahren verwendet, bei dem der gesamte Server als Image gesichert wird. Es wird dazu keine Netzwerkverbindung zwischen Datensicherungssystem und Cloud-Server oder administrative Accounts in den zu sichernden Cloud-Servern benötigt. Dadurch kann eine hohe Sicherheit bei der Durchführung der Datensicherung gewährleistet werden. Die Datensicherungen werden 5x wöchentlich durchgeführt. Die Wiederherstellung wird nach Aufwand berechnet. Die Datensicherungen werden 14 Tage vorgehalten.

5. Monitoring

5.1. Die Cloud-Server werden durch VMware vCenter und VMware Monitoring Systeme 24x7x365 überwacht. Überwacht werden dabei die Ressourcen (CPU, RAM, Netzwerk, Disk) sowie die für den Betrieb der Server notwendige Infrastruktur. Zusätzlich werden von tisoware bestimmte Überwachungsfunktionen für bestimmte Dienste wie TomCat, Datentransfer von und zu den Buchungsterminals, Datentransfer zu Exchange sowie dem Email Versand kontinuierlich ausgeführt. Falls erforderlich werden diese Dienste neu gestartet.

6. Support

6.1. Der Support umfasst Unterstützung während der Servicezeit (üblicherweise Mo - Do, 08:00 Uhr – 17:00 Uhr; Fr, 08:00 Uhr – 16:00 Uhr). Gesetzliche Feiertage in Bayern und Baden-Württemberg, der 24.12. und der 31.12. sowie vorher bekannt gemachte Wartungsfenster sind von der Servicezeit ausgenommen.

7. Wartungsfenster

7.1. Wartungsfenster finden außerhalb der regulären Servicezeiten nach Vorankündigung statt. Bei wichtigen Gründen kann ein Wartungsfenster auch kurzfristig zu jeder Zeit angekündigt und durchgeführt werden. tisoware 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 Verbindungen werden mittels modernster Firewalls überprüft, überwacht und ggf. abgelehnt und protokolliert. Es werden nur die notwendigen Ports, Protokolle und Dienste freigeschalten. Mittels VPN-Verbindung (Site-to-Site) erfolgt eine Authentifizierung an der Core-Firewall und die Verbindung zum Zielserver / Zielnetzwerk. Die Verfügbarkeit von VPN Verbindungen ist grundsätzlich abhängig von der gewählten tisoware Edition –vgl. auch Feature Matrix. Web-Zugriffe über HTTP(S)- Verbindungen werden durch die WAF (Web-ApplicationFirewall) entgegengenommen. Hiernach erfolgt eine Prüfung gegen Security-Profile und das Routing zu den Ziel-Ressourcen.

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 tisoware freigegebenen Browser auf Kundenseite voraus. Hierzu verweisen wir auf die Umgebungsrichtlinien der jeweils einzusetzenden tisoware-Version.