Anhang A - Technische Voraussetzungen

Die folgenden technischen Voraussetzungen sind für die Nutzung der Software vom Kunden einzuhalten bzw. zu schaffen und während der Vertragslaufzeit aufrechtzuerhalten:

1. Unterstützte Browser

Für den Zugriff auf die Benutzeroberfläche der Software empfehlen wir die Verwendung der folgenden Browser:

- Mozilla Firefox,
- Google Chrome,
- Microsoft Edge oder
- Apple Safari

in der jeweils neuesten Version. Grundsätzlich nicht unterstützt werden Browser-Versionen, die vom Browser-Hersteller nicht mehr supportet werden.
In der Konfiguration muss die Ausführung von JavaScript sowie das Einblenden von Pop-Up-Fenstern erlaubt sein und bei der Verwendung des Internet Explorers muss zusätzlich der Kompatibilitätsmodus deaktiviert sein.

2. Monitor-Auflösung

Die Benutzeroberfläche der Software erfordert eine Mindestauflösung des Monitors von 1920 x 1080 Pixeln (HD-Format) für eine ideale Ansicht.
Bei geringerer Auflösung kann die vollständige Bedienbarkeit, z.B. durch Nicht-Darstellung von Bedienelementen, nicht komplett gewährleistet werden. Obwohl der automatisch anpassende Modus (Responsive Design) eine Darstellung grundsätzlich auf jedem Display ermöglicht sind gerade Tabellen auf kleinen Displays nur eingeschränkt nutzbar.

3. Internet-Anbindung

Eine ausreichende Arbeitsgeschwindigkeit wird von vielen Faktoren beeinflusst. Neben der genutzten Infrastruktur (Festnetz/Mobil) für den Zugriff auf das Internet sind auch die jeweils übertragene Datenmenge und die Komplexität der Software, z.B. der zeitgleiche Systemzugriff verschiedener Nutzer, einfließende Parameter. Eine allgemeine Mindestanforderung an die Bandbreite einer Internetanbindung ist von daher kaum zu definieren.

4. Passwort Richtlinie

Aus Sicherheitsgründen muss jeder Nutzer der Software ein Passwort wählen, welches den üblichen Sicherheitskriterien entspricht. Entsprechende Regelwerke werden beim Setzen des Passwortes durch die Software vorgegeben, wenn der Kunde diese konfiguriert hat. Der bewusste Umgang mit persönlichen und sicherheitsrelevanten Zugangskennungen liegt in der Verantwortung jedes einzelnen Benutzers, bzw. in der Konfiguration des Kunden. So wird empfohlen alle in der Software möglichen Sicherheitsoptionen zu nutzen.
Mehrfache vergebliche Falscheingaben des Passwortes führen zur Sperrung des Nutzer-Kontos, wenn die Einstellung vom Kunden konfiguriert wurde.

5. Spam und Cookies

Die Software bietet Konfigurationsmöglichkeiten zur Umsetzung von Sicherheitsmechanismen wie zum Beispiel Captcha Formular Schutz. Diese können nach Wahl vom Kunden konfiguriert werden und erfordern nach Aktivierung evtl. Anpassungen um den Datenschutzbestimmungen zu entsprechen.