1. Systembeschreibung

1.1 Software as a Service

Unter "Software as a Service" (kurz SaaS) wird die Bereitstellung eines Kernservices und zusätzlicher Services im Zusammenhang mit den Kern-Systemen (butler, comp.ASS) des Auftragnehmers verstanden, die ein Auftraggeber im zugehörigen SaaS Vertrag gebucht hat. Im Hostingverfahren werden über eine Datenverbindung (Internet) die Softwarelösungen des Auftragnehmers beim Auftraggeber bereitgestellt. Diese Bereitstellung erfordert je nach gebuchter Servicekombination die Erfüllung von speziellen Systemvoraussetzungen und Installationen. Der Auftraggeber hat die technischen Anforderungen zur Nutzung des Clients oder Browsers für den Zugriff auf die zur Nutzung der bereitgestellten Software zu erfüllen, über die im Folgenden aufgeklärt wird. Verschiedene Zusatzservices hängen u. a. von unterschiedlichen Randfaktoren ab, die der Auftragnehmer nicht zu vertreten hat. So ist beispielsweise der Auftraggeber für die Anbindung seiner Clients an das Datennetz (Internet) selbst verantwortlich, während der Auftragnehmer seinerseits den Übergabepunkt in das Datennetz (Internet) zu pflegen hat.
Der Auftragnehmer hält die eingesetzte Software auf dem Stand der anerkannten Regeln der Technik.

1.2 Rechenzentrum von prosozial

Das prosozial Rechenzentrum befindet sich in Koblenz (Deutschland) und ist entsprechend den Vorgaben nach der EU DSGVO Artikel 5 Abs 1 e),f) Artikel 28 , 32 ff gesichert. Die Daten werden u. a. in einer Microsoft SQL Server Datenbank betrieben. Die Dokumente im Dokumentenmanagementsystem (DMS) werden chaotisch, speicherarm und nach Möglichkeit einmalig (jedoch mehrfach vernetzbar) bevorzugt im Format PDF abgelegt. Die derzeitige Bereitstellung der butler 21 Software erfolgt über die Microsoft Remote Desktop Services (RDP) als „Remote App“. prosozial setzt auf Technologien der Firma Microsoft.

1.3 Bereitstellung des Basispaketes und weiterer Services über die „Remote-App“

Der Funktionsumfang der butler 21 Softwarelösung wird dem Auftraggeber mittels einer „Remote-App“, die auf den Clientgeräten des Auftraggebers einzurichten ist, bereitgestellt. Vereinfacht dargestellt erhält der jeweilige Anwender über eine gesicherte technische Verbindung Zugang zum Rechenzentrum des Auftragnehmers. Dieser Zugang ist zur gleichen Zeit nur von einem Anwender auf einem Gerät nutzbar. Die Softwarelösung wird im Rechenzentrum des Auftragnehmers ausgeführt und die Anzeige-, Eingabe- und Ausgabedaten werden über die verschlüsselte Verbindung übertragen. Nach einer Stunde Inaktivität kann durch den Auftragnehmer diese "Remote App" automatisch abgemeldet werden. Durch Service-Levels werden die Zeitintervalle zur Abmeldung konkretisiert. Eine Neuanmeldung ist jederzeit möglich. Nicht gespeicherte Tätigkeiten gehen verloren. Jeder Anwender erhält zur Nutzung der "Remote App" einen eigenen personalisierten Zugang, mit dem die Authentifizierung durchgeführt wird. Bei Verlust der Zugangsdaten oder bei Verdacht auf Missbrauch durch Dritte ist dies unverzüglich der Kundenbetreuung anzuzeigen (siehe auch Ziffer 11).

1.4 Empfohlene Geräte

Der Auftragnehmer listet unterstützte als auch empfohlene Geräte wie bspw. Laptops, Tablets, Drucker etc. aktuell unter https://saas.prosozial.de auf.

1.5 Supporttools

Für den Support während der ServiceLine- oder technischen Hotlineleistungen wird seitens des Auftraggebers die Verwendung der Anwendung "Remotehilfe" unter Windows 10 vorausgesetzt. Für administrative Tätigkeiten wird das Fernwartungstool "GoToAssist" (https://fastsupport.gotoassist.com) verwendet. So können wir eine optimale Leistungserbringung im Supportfall gewährleisten.

1.6 Datensicherungen

Aufgrund der Massnahmen zur physischen und organisatorischen Datensicherheit (Hardwareraid und Redundanzen sowie Rechtestruktur) ist von einem Datenverlust nicht auszugehen. Für den Fall eines Desaster Recovery sind folgende Massnahmen getroffen.

Im Rechenzentrum der prosozial GmbH werden täglich die Datenbanken und Dateien der Kunden gesichert.

Die dazu nötige Hardware befindet sich in einem anderen Brandabschnitt des Gebäudes, um auch im Brandfall die Existenz eines Backups zu garantieren. Ab 20 Uhr werden dazu täglich sämtliche Daten verschlüsselt auf den Backupservern abgelegt.

Die Tagessicherungen werden für 31 Tage gehalten. Sollte aufgrund eines unvorhersehbaren Fehlers ein Datenverlust auftreten, kann so schnellstmöglich ein aktueller und konsistenter Datenstand wiederhergestellt werden.

Am Ende eines Monats wird ein kompletter Datensatz auf Bandlaufwerke geschrieben. Diese werden extern aufbewahrt, um auch im Falle eines Verlustes des kompletten Gebäudes eine Wiederherstellung der Daten zu gewährleisten. Diese Monatssicherungen werden für 1 Jahr vorgehalten.

Die letzte Monatssicherung des Jahres wird entsprechend den gesetzlichen Aufbewahrungsfristen eingelagert und aufbewahrt.

1.7 Exit-Management

Im Falle einer erfolgten und bestätigten Kündigung stellt der Auftragnehmer dem Auftraggeber nach Beauftragung durch den Auftraggeber eine Sicherung der Daten und des DMS zur Verfügung. Die Beauftragung zur Bereitstellung dieser Datensicherung hat spätestens 2 Monate nach Kündigung zu erfolgen. Die Daten werden auf einem Speichermedium verschlüsselt ausgeliefert. Das Kennwort zur Entschlüsselung wird dem Auftraggeber separat zur Verfügung gestellt. Die Kosten für den Aufwand sind vom Auftraggeber zu tragen und werden nach geleistetem Aufwand berechnet. Die Daten auf dem Rechenzentrum können durch den Auftragnehmer 3 Monate nach Ende des Vertrages gelöscht werden. Eine Aufbewahrungspflicht der Kundendaten durch den Auftragnehmer nach Kündigung besteht nur nach ausdrücklicher schriftlicher Vereinbarung. Nach Entlastung durch den Auftraggeber kann eine Löschung jederzeit schriftlich beauftragt werden.

1.8 Speicherverhalten

Die Daten des Auftraggebers werden einerseits in einer Microsoft SQL Server Datenbank, sowie im Dokumentenmanagementsystem gespeichert.
Dateien werden beim ein- und auschecken automatisch versioniert gespeichert. Somit entsteht evtl. ein Mehrbedarf an Speicher, der über Speicherservices abzudecken ist. Pro genutztem Gigabyte kann der Auftragnehmer dem Auftraggeber monatlich Kosten in Rechnung stellen.

1.9 Kennwortrichtlinie

Es ist ein sicheres Kennwort für den Benutzerzugang zum Rechenzentrum zu verwenden. Die Kennwortrichtlinien erfordern ein sicheres Passwort (von zurzeit mindestens 9 Zeichen Länge, wovon mindestens je 1 Zeichen aus 3 der 4 Kategorien – Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen – bestehen muss). Der Auftragnehmer ist berechtigt, in eigenem Ermessen die Kennwortrichtlinien zur Gewährleistung des Sicherheitsniveaus zu ändern. Der Auftraggeber wird hierüber rechtzeitig vorab informiert. Benutzer können das Passwort unter folgender Adresse ändern:
https://rzp.hilfeprodukte.de/RDWeb/Pages/de-DE/password.aspx

2. Systemvoraussetzungen für die Servicenutzung

Folgend werden die entsprechenden Systemvoraussetzungen an die Hard- und Software des Auftraggebers beschrieben, um die im Vertrag gebuchten Services seitens des Auftraggebers verwenden zu können.

2.1 Voraussetzungen für die Nutzung des Kernservices "Remote App"

Zur Nutzung von butler 21 im Hostingverfahren mittels der "Remote App" sind derzeit folgende Mindestvoraussetzungen an dem jeweiligen Gerät zu erfüllen (aktuell verbindlich unter https://saas.prosozial.de).

2.1.1 Microsoft RDP 8 kompatibler Client

Unterstützt werden vom Auftragnehmer zurzeit die RDP 8 Clients mit Windows 8.1 und mit Windows 10 (jeweils aktueller Patch Stand). Die Angaben beziehen sich auf diese Systeme und werden daraufhin optimiert.
Unterstützungen zu anderen Clients werden vom Auftragnehmer grundsätzlich kostenpflichtig als Dienstleistung ohne Funktionsgarantie geleistet, von einer Expertise der Fremdsysteme kann seitens des Auftragnehmers nicht ausgegangen werden.
Die "Remote App" arbeitet nur über eine sichere und verschlüsselte Verbindung.
Der Zugriff erfolgt entweder über eine RDP-Verknüpfung oder in Ausnahmen auch per Webbrowser (URL: https://rzp.hilfeprodukte.de/RDWeb), womit die Remote App gestartet wird. Aktuelle Installations-Anleitungen werden unter https://saas.prosozial.de veröffentlicht. Bei Zugriff per Webbrowser und URL ist ein aktueller Browser (z. B. Internet Explorer Version 11 oder höher) erforderlich.

2.1.2 Internetverbindung

Die Verbindung zum Rechenzentrum von prosozial wird über einen Internetzugang hergestellt, der seitens des Auftraggebers für dessen Clients verfügbar gehalten werden muss, um den Remote App Service nutzen zu können.

Die empfohlene Mindestvoraussetzung der Internetverbindungsgeschwindigkeit lautet gegenwärtig:

- Upload: 1000 Kbit/s
- Download: 6000 Kbit/s

Jeweils aktuelle empfohlene Internetverbindungsgeschwindigkeiten werden unter https://saas.prosozial.de veröffentlicht. Die erforderliche Internetverbindungsgeschwindigkeit ist abhängig vom Nutzungsverhalten (Scannen, Drucker etc.), von der Anzahl der gleichzeitigen Nutzerzugriffe über die Internetanbindung sowie vom jeweiligen Arbeitsverhalten und der Organisationsstruktur. Der Auftragnehmer kann im Rahmen der Angebotsphase zusammen mit dem Auftraggeber prüfen, ob die beim Auftraggeber entsprechend erforderliche Internetverbindungsgeschwindigkeit sowie akzeptable Reaktionszeiten verfügbar sind und ob eine Nutzung der Serviceangebote des Auftragnehmers unter Berücksichtigung dieser Rahmenbedingungen sinnvoll ist.

2.1.3 Anforderungen an die Nutzerkennung

Die Nutzerkennung erfordert eine gültige E-Mail Adresse und ein sicheres Kennwort. Bei Verlust des Kennworts ist die Wiederherstellung des Zugangs nur über diese E-Mail Adresse möglich.

2.2 Allgemeine Systemvoraussetzungen

2.2.1 Lautsprecher / Kopfhörer

Zur Nutzung von z. B. Hilfefilmen sind Lautsprecher oder Kopfhörer erforderlich.

2.2.2 Aktueller Internetbrowser

Um Internetadressen aufrufen zu können, wird lokal beim Client des Auftraggebers ein aktueller Internetbrowser z. B. Microsoft Edge benötigt.

Zusätzlich können Services, die ein mobiles Arbeiten unterstützen, auf einen aktuellen Internetbrowser angewiesen sein.

2.3 Servicebezogene Systemvoraussetzungen

2.3.1 Voraussetzungen für den Service E-Mail-Dienst

Für die Integration von E-Mails in butler 21 werden gegenwärtig folgende E-Mail Provider unterstützt:

- Microsoft Office 365 "Exchange Online"
- Microsoft Konto (Dienst von Microsoft Outlook.com / Live.de / Outlook.de)
- Deutsche Telekom
- GMX
- Web.DE

E-Mails werden per gesicherter POP3 und SMTP Verbindung (SSL) abgeholt und versendet. Die Größe von ein- und ausgehenden E-Mails ist begrenzt, in der Regel auf 25 MB pro E-Mail. Zusätzlich gelten die jeweiligen Begrenzungen der jeweiligen E-Mail Provider.
Für die Integration dieses Services sind jedoch stets die Details des E-Mailsystems des Auftraggebers zu prüfen. Eine danach folgende anzupassende Anbindung des E-Mail Services, die von den bisherigen Standards des Auftragnehmers abweicht, ist ggf. separat zu projektieren und kann Entwicklungs- oder Einrichtungskosten verursachen, die der Auftraggeber nach Beauftragung zu tragen hat.
Abgerufene E-Mails werden durch den prosozial Mailservice spätestens nach 30 Tagen vom E-Mail-Server (Posteingang des Postfachs) gelöscht. Wünscht der Auftraggeber eine weitere Sicherung der E-Mails außerhalb von butler / comp.ASS, liegt dies in der Verantwortung des Auftraggebers.

2.3.2 Voraussetzungen für den Service Fax-Dienst

Bei Buchung des Fax-Dienstes erhält der Auftraggeber eine Rufnummer aus dem Koblenzer Ortsnetz zugeteilt, über die gesendet und empfangen wird. Zur weiteren Empfangsnutzung einer beim Auftraggeber vorhandenen Rufnummer müssen in beim Auftraggeber genutzten und relevanten Fax-Geräten Rufumleitungen auf diese neue Nummer eingerichtet werden.

2.3.3 Voraussetzungen für Tele-Services im Rahmen von Serviceline und Hotline

Der Auftraggeber hat sicherzustellen, dass das vereinbarte Support-Tool bei seinen zu verantwortenden Clientgeräten eingesetzt werden kann. Dafür ist es erforderlich, dass mindestens die Windows Remotehilfe funktioniert. Weitere Einzelheiten sind auf der Internetseite https://saas.prosozial.de bereitgestellt.
Ist dieser vorab genannte Supporttool durch den Auftraggeber nicht nutzbar, ist separat festzulegen, wie der Auftragnehmer einen technischen Zugang vom Auftraggeber auf die vom Auftragnehmer zu supportenden Geräte eingeräumt bekommt.

2.3.4 Voraussetzungen für die Nutzung von Portal-Services im Browser

Zur Nutzung der Portal-Services zur erweiterten mobilen Arbeit sind nachfolgende Voraussetzungen zu erfüllen:

- vorhandene butler 21 Systemanmeldung;
- ein üblicher in Deutschland verfügbarer aktueller Internet-Browser (z. B. Microsoft Edge);
- eine stabile Internet Verbindung für die Nutzung der Inhalte.

2.3.5 Voraussetzungen für die Nutzung der Windows App "Wissen 21"

Zur Nutzung der Windows App „Wissen 21“ sind nachfolgende Voraussetzungen zu erfüllen:

- Es ist ein aktuelles Microsoft Windows 8.1 / Windows 10 Betriebssystem erforderlich.
- Es ist eine Internetverbindung, um Inhalte zu erhalten, erforderlich. Inhalte werden teilweise offline verfügbar gemacht und gehalten. Ohne eine bestehende Internetverbindung finden keine Aktualisierungen statt.
- Die Installation erfolgt über den Windows Store (Suchwort im Store "prosozial";
  URL: https://saas.prosozial.de)
- Es ist ein prosozial Konto erforderlich.

- Es ist ein Microsoft-Konto erforderlich.

2.3.6 Voraussetzungen für die Microsoft Office 365 Integration

Der Auftraggeber ist verantwortlich für den Abschluss des Microsoft Office 365 Vertrags inkl. Auftragsdatenverarbeitungsvertrag mit der Firma Microsoft. Hierzu kann der Auftraggeber auch auf Vermittlungsservices des Auftragnehmers zurückgreifen.
Der Auftragnehmer ist durch den Auftraggeber mit der delegierten Administration zu beauftragen. Dazu wird die Partner ID der Firma prosozial hinterlegt: **1047764**
Der Auftragnehmer wird mit der gesamten Abwicklung gegenüber Microsoft beauftragt und handelt dann im Namen des Auftraggebers.
Um die einzelnen Dienste nutzen zu können, ist es erforderlich, dass die entsprechenden Zugangsdaten in den Registrierungen des butler 21 hinterlegt sind. Für die ordnungsgemäße Hinterlegung ist der Auftraggeber verantwortlich.

2.3.7 Voraussetzungen für Geo-Redundanz-Sicherung

Wenn im SaaS-Vertrag eine georedundante Datensicherung beauftragt wurde, muss der Auftraggeber dazu für den Auftragnehmer einen Speicherort bereitstellen. Eine Möglichkeit würde beispielsweise eine Lösung über Office 365 darstellen.

2.3.8 Voraussetzungen für Domain-Integration

Zur Gewährleistung einer ordnungsgemäßen Integration einer Domain, die entweder über den Auftragnehmer oder den Auftraggeber beschafft worden ist, in die Systemumgebung der Kernsysteme des Auftragnehmers (butler / comp.ASS), ist es erforderlich, dass der Auftraggeber dem Auftragnehmer die bestehende E-Mail-Systemlandschaft (soweit erforderlich) beschreibt und Änderungen in der E-Mail-Systemlandschaft dem Auftragnehmer rechtzeitig zuvor anzeigt (siehe auch Ziffer 2.3.1).

2.3.9 Voraussetzungen für Web-Präsenz

Voraussetzung für die Nutzung von Web-Präsenz-Services ist, dass die zugehörige Internet-Domain über den Auftragnehmer vermittelt und verwaltet wird.
Hinweis: Bei Einstellung der Zahlung und Nutzung des Domain-Services (Vermittlung und Verwaltung einer Domain durch den Auftragnehmer für den Auftraggeber) stellt der Auftragnehmer auch seine Leistungen ein. Das bedeutet, dass die Domain dauerhaft neu vergeben werden könnte, worauf der Auftragnehmer keinen Einfluss hat.

2.4 Voraussetzungen für die Wahrung der Datensicherheit

Der Auftragnehmer speichert die Daten im Rechenzentrum in Koblenz und schützt die Daten gegen Schadsoftware. Damit dies durchgängig gewährleistet werden kann, müssen auch die Endgeräte des Auftraggebers entsprechend geschützt werden. Somit ist es mindestens erforderlich, dass der Auftraggeber einen aktuellen Virenscanner und eine entsprechende Firewall auf den betroffenen Geräten installiert hat und den Status der darauf laufenden Programme überwacht. Im Windows Sicherheitscenter / Wartungscenter ist

es erforderlich, dass keine sicherheitsrelevanten Warnungen ignoriert werden. Weiterhin ist es erforderlich, dass technische Sicherheitsmaßnahmen von Microsoft beibehalten werden, wie bspw. die "User Access Control" / Benutzerkontensteuerung (kurz UAC) darf nicht deaktiviert werden. Zum Schutz des Rechenzentrums setzt der Auftragnehmer Kontrollmechanismen zur Überwachung des Sicherheitsstatus der Endgeräte ein. Der Auftragnehmer behält sich das Recht vor, inkompatible bzw. von Viren infizierte Endgeräte von der Nutzung der gebuchten Services zum beiderseitigen Schutze auszuschließen. Aktuelle Sicherheitshinweise hierzu werden auf der Internetseite https://saas.prosozial.de durch den Auftragnehmer veröffentlicht. Sollte eine allgemeine, akute Gefahr für die Datensicherheit bestehen, sind die erforderlichen sicherheitsrelevanten Maßnahmen sowohl vom Auftragnehmer als auch vom Auftraggeber umzusetzen.
Weiterhin können als infiziert erkannte Dateien, die in das Rechenzentrum vom Auftragnehmer (selbstständig oder von extern, bspw. per E-Mail) hinzugefügt werden sollen, automatisch und ohne Rückmeldung an den Verursacher gelöscht werden, wenn dies technisch notwendig erscheint.

3. Anpassungen an Systemvoraussetzungen / Systembeschreibung

Die Services des Auftragnehmers sollen den aktuellen Anforderungen und den anerkannten Regeln der Technik ständig genügen. Um im Fluss zu bleiben, werden die Systemvoraussetzungen entsprechend, z. B. wegen neuer Technologien, Entwicklung neuer Services etc. durch den Auftragnehmer angepasst. Hierfür bedarf es keiner Aktualisierung des Vertrages. Sofern sich Änderungen ergeben, wird der Auftraggeber möglichst frühzeitig informiert. Aktuelle Informationen rund um das Rechenzentrum sind auf https://saas.prosozial.de abrufbar.