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 BDSG §9 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 Kern-Systeme 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 oder comp.ASS 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.

1.4 Empfohlene Geräte

Der Auftragnehmer listet unterstützte als auch empfohlene Geräte wie bspw. Notebooks, Tablets, Drucker, Scanner, etc. aktuell unter saas.prosozial.de auf.

1.5 Teleservice

Für die Serviceline- oder Hotlineleistung wird seitens des Auftragnehmers auf Teleservicefunktionalitäten im Rahmen von Microsoft Teams zurückgegriffen. Der Teleservice Microsoft Teams wird dabei als Kommunikationsplattform und Supportplattform genutzt, um eine optimale Leistungserbringung zu gewährleisten.

1.6 Datensicherungen

Im Rechenzentrum Koblenz werden die Daten des Auftraggebers so verarbeitet, dass von einem technischen Datenverlust nicht auszugehen ist. Der Auftraggeber muss keine separaten Datensicherungen durchführen.

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 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.

Es ist dabei zu beachten, dass Dateien, die ein- und ausgecheckt werden, versioniert gespeichert werden. 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. Dies kann über Speicherservice-Pakete separat geregelt sein.

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 / comp.ASS 21 im Hostingverfahren mittels der "Remote App" sind derzeit folgende Mindestvoraussetzungen an dem jeweiligen Gerät zu erfüllen (aktuell verbindlich unter https://saas.prosozial.de/remote-app).

2.1.1 Microsoft RDP 8.1 kompatibler Client

Unterstützt werden vom Auftragnehmer zurzeit die RDP 8.1 Clients mit Windows 8.1, Windows 10 oder Windows 11 (jeweils aktueller Patch Stand). Die Angaben beziehen sich auf diese Systeme und werden daraufhin optimiert.

Unterstützungen zu anderen Client-Betriebsystemen 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 (SSL).

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/downloads 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 empfohlenen Internetverbindungsgeschwindigkeiten sind gegenwärtig:

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

Jeweils aktuelle empfohlene Internetverbindungsgeschwindigkeiten werden unter 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 oder Google Chrome (jeweils aktuelle Version) 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 / comp.ASS 21 werden gegenwärtig folgende E-Mail Provider unterstützt:

- Microsoft Office 365 "Modul Exchange"
- 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.

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 Teleservices im Rahmen von Serviceline und Hotline

Der Auftraggeber hat sicherzustellen, dass der vereinbarte Teleservice bei seinen zu verantwortenden Clientgeräten eingesetzt werden kann. Dafür ist es erforderlich, dass mindestens die Microsoft Teams Web App funktioniert. Weitere Einzelheiten sind auf der Internetseite https://saas.prosozial.de/support bereitgestellt.

Ist dieser vorab genannte Teleservice 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 SAM Services im Browser

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

- vorhandene butler 21 / comp.ASS 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").
- Es ist ein prosozial Konto erforderlich.

2.3.6 Voraussetzungen für die Microsoft 365 Integration

Der Auftraggeber ist verantwortlich für den Abschluss des Microsoft 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 / comp.ASS 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.

2.3.9 Voraussetzungen für Web-Präsenz / Web-Visitenkarte

Voraussetzung für die Nutzung von Web-Präsenz- und Web-Visitenkarten-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 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.