Vereinbarung
über die Verarbeitung personenbezogener Daten
(Auftragsverarbeitung gemäß Art. 28 DSGVO)

zwischen

dem Empfänger des vorstehenden Angebotes

- nachstehend Auftraggeber genannt -

und

Sage GmbH
Franklinstraße 61-63
60486 Frankfurt am Main

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

Diese Vereinbarung konkretisiert die gesetzlichen Rechte und Pflichten, die sich für die Vertragsparteien aus dem anwendbaren Datenschutzrecht und insbesondere aus dem Bundesdatenschutzgesetz, aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DSGVO“) sowie der nationalen Datenschutzgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet. Sie findet Anwendung auf alle Tätigkeiten, die mit dem / den Hauptvertrag / Hauptverträgen (im Einzelnen im Anhang Produkte aufgeführt) in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Als solche Tätigkeiten kommen insbesondere ein Direkt- oder Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump / Backup-Datei – vor allem im Zusammenhang mit Support- und Consultinganfragen – in Betracht, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des / der Hauptvertrages / Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf mit dem Laufzeitende des letzten verbleibenden, im Anhang Produkte aufgeführten Hauptvertrages.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Verarbeitung: Verarbeitung umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die

Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete dokumentierte Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in dokumentierter Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich

(1) Der Auftragnehmer prüft und wartet automatisierte Verfahren oder Datenverarbeitungsanlagen im Auftrag, insbesondere die von ihm im Rahmen eines getrennten Vertragsverhältnisses überlassene Standardsoftware und bietet im Rahmen seiner Serviceangebote weitergehende Hilfestellungen im Umgang mit der Software an. Ferner bietet er Softwareprodukte auch im Rahmen von Hosting, ASP, SaaS oder Cloud basierender Angebote an. Im Rahmen dieser Tätigkeiten kann in besonderen Konstellationen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die umfassten Tätigkeiten sind in der Leistungsbeschreibung des / der Hauptvertrages / Hauptverträge konkretisiert. Der / Die Hauptvertrag / Hauptverträge sind ferner im Anhang Produkte zu dieser Vereinbarung, unter Nennung der jeweils betroffenen Datenkategorien, aufgeführt. Die Auflistung wird von den Parteien bei Wegfall oder Neuabschluss eines weiteren Hauptvertrages, der auch Auftragsverarbeitung zum Gegenstand hat, fortlaufend aktualisiert.

(2) Die nach diesem Vertrag den Parteien auferlegten Rechte und Pflichten gelten nur während der Laufzeit des Vertrages und innerhalb dieses Zeitraums nur in den Zeitabschnitten bei denen tatsächlich eine Auftragsverarbeitung durchgeführt wird oder eine vergleichbare Gefahrenlage für personenbezogene Daten, für die der Auftraggeber verantwortlich ist, gegeben ist.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Darüber hinaus kann sich im Einzelfall für den Auftragnehmer eine gesetzliche Verpflichtung zur Verarbeitung personenbezogener Daten ergeben. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die betreffende rechtliche Verpflichtung verbietet eine solche Mitteilung wegen wichtigen öffentlichen Interesses.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des anwendbaren Datenschutzrechts gerecht wird. Er wird die geeigneten und gesetzlich erforderlichen technischen und organisatorischen Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet insbesondere

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Darstellung der technischen und organisatorischen Maßnahmen des Auftragnehmers ist diesem Vertrag als Anhang TOM beigefügt.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigtenverhältnisses zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

(4) Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und teilt dem Auftraggeber dessen Kontaktdaten mit (siehe Anhang TOM).

(5) Im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen unterstützt der Auftragnehmer den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der gesetzlichen Pflichten, die den Auftraggeber als Verantwortlichen treffen (u.a. bei der Wahrnehmung von Betroffenenrechten, der Durchführung von Kontrollen durch die zuständige Datenschutzaufsichtsbehörde sowie bei der Erfüllung gesetzlicher Informationspflichten gegenüber Betroffenen und Datenschutzbehörden).

(6) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und dem Auftraggeber auf Verlangen in geeigneter Weise nachzuweisen.

(8) Die Auftragsverarbeitung findet innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Eine Verlagerung in ein Drittland außerhalb dieses Gebietes ist unter Einhaltung der in Art. 44 ff DSGVO festgelegten Bedingungen zulässig. Einzelheiten regelt § 6 und hier insbesondere Abs. 4.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne des anwendbaren Datenschutzrechts für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer verantwortlich (Verantwortlicher). Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber.

(2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen (Einzelweisung). Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden.

(3) Der Auftraggeber ist für die Wahrung der Betroffenenrechte verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund von angeblich unrechtmäßigen Datenverarbeitungen Ansprüche geltend machen, wird der Auftraggeber, soweit diese angeblich unrechtmäßigen Verarbeitungen auf Vorsatz oder Fahrlässigkeit des Auftraggebers beruhen, den Auftragnehmer von allen solchen Ansprüchen freistellen. Soweit vom Leistungsumfang im Hauptvertrag / in den Hauptverträgen umfasst, wird der Auftragnehmer den Auftraggeber nach dokumentierter Weisung bei der Erfüllung der Ansprüche Betroffener unterstützen (insbesondere hinsichtlich Berichtigung, Löschung und Sperrung von Daten).

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 5 Kontrollrechte und -pflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Die hierfür erforderlichen Informationen werden dem Auftraggeber gemäß nachfolgendem Absatz zur Verfügung gestellt.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag geregelten Pflichten zur Verfügung. Er ermöglicht und trägt bei zu Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

(3) Die Häufigkeit der Kontrollen soll maximal einmal jährlich erfolgen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt durch eine Vor-Ort Kontrolle durch die Vorlage eines geeigneten Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revisor, interner oder externer Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor) oder einer geeigneten Datenschutz-Zertifizierung durch eine zugelassene Stelle erbracht werden ("Zertifizierungsurkunde"). Die Zertifizierungsurkunde muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anhang TOM zu überzeugen.

§ 6 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, die im Anhang Produkte benannten, weiteren Auftragsverarbeiter (Subunternehmer) einschaltet. Über eine Änderung der genannten oder die Hinzuziehung weiterer Subunternehmer wird der Auftragnehmer den Auftraggeber in Textform rechtzeitig informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Der Auftraggeber kann bei Vorliegen sachlicher Gründe der Unterbeauftragung innerhalb von 4 Wochen nach Kenntnisnahme in Textform widersprechen. Im Fall der Einschaltung von im Sinne der §§ 15 ff. AktG mit dem Auftragnehmer verbundenen Unternehmen als Subunternehmer erteilt der Auftraggeber hiermit schon jetzt ausdrücklich seine Zustimmung.

(3) Der Auftragnehmer wird weiteren Auftragsverarbeitern vertraglich dieselben Pflichten wie nach diesem Vertrag auferlegen, einschließlich hinreichender Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen.

(4) Ist ein weiterer Auftragsverarbeiter in einem Drittland ansässig, wird der Auftragnehmer die in Art. 44 ff DSGVO niedergelegten Bedingungen einhalten. Neben einer Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO) kann diese auch vorbehaltlich geeigneter Garantien erfolgen, wobei Art. 46 Abs. 2 lit c) DSGVO Standarddatenschutzklauseln zur Anwendung kommen.

§ 7 Informationspflichten

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne des anwendbaren Datenschutzrechts liegen.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

§ 8 Vertragsdauer und -beendigung

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des letztbestehenden Hauptvertrages.

(2) Nach Abschluss der Erbringung der Verarbeitungstätigkeiten bzw. nach Beendigung der Vereinbarung hat der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen oder herauszugeben. Dies gilt nicht, soweit für den Auftragnehmer auf Grundlage des anwendbaren Datenschutzrechts eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z.B. gesetzliche Aufbewahrungspflicht).

(3) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und / oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

§ 9 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anhängen im Fall von Änderungen, Anpassungen und / oder Ergänzungen datenschutzrechtlicher Bestimmungen

– insbesondere der DSGVO und / oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Soweit der Auftragnehmer den Auftraggeber gemäß § 3 Abs. 5 bzw. § 4 Abs. 3 dieser Vereinbarung unterstützt oder der Auftraggeber dem Auftragnehmer gemäß § 4 Abs. 2 bzw. § 8 Abs. 3 dieser Vereinbarung ergänzende Weisungen erteilt und hierdurch Aufwände anfallen, die unverhältnismäßig oder nicht vom Leistungsumfang im Hauptvertrag / in den Hauptverträgen gedeckt sind, wird der Auftragnehmer dies im Vorfeld der Umsetzung dem Auftraggeber mitteilen. Besteht der Auftraggeber dennoch auf der Umsetzung, kann der Auftragnehmer die Durchführung von einer Kostenübernahmezusage des Auftraggebers abhängig machen.

(4) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Ausschließlicher Gerichtsstand ist Frankfurt am Main.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Diese AV-Vereinbarung wird mit Unterzeichnung des vorstehenden Angebotes gültig.

Anhang: Produkte Sage People

Hauptvertrag	Betroffene Datenkategorien und Personen *	Subunternehmer / Standort der Datenverarbeitung / erbrachte Teilleistungen **
Sage People		A
People Management	1, 2, 3, 4, 5, 6, 14	
Attendance & Leave Management	1, 7, 11, 12, 14	
Payroll Compensation & Benefits	1, 3, 7, 8, 14, 15	
Performance & Talent Management	1, 7, 10, 14	
HR & People Analytics	1, 6, 7, 11, 14	
Talent Acquisition	1, 2, 3, 9, 12, 13, 14	
Sage People Recruiting	1, 2, 5, 8, 9, 13	A
OCR	13	B

* Datenkategorien und Personen:

1. Personenstammdaten (z.B. Name, Titel, Geburtsdatum, Geschlecht, Anschrift) von Mitarbeitern und Bewerbern
2. Kommunikationsdaten (z.B. Telefon, Nebenstelle, Fax, E-Mail, IP-Adresse) von Mitarbeitern und Bewerbern
3. Daten in Zusammenhang mit der Lohn- und Gehaltsabrechnung (z.B. Familienstand, Schwerbehinderungsgrade, Beruf, Religion, Nationalität) von Mitarbeitern
4. Steuer- und sozialversicherungsrechtliche Daten (z.B. Steuernummer, Krankenversicherung) von Mitarbeitern
5. Kontoverbindungsdaten von Mitarbeitern und ggfls. Bewerbern
6. Vertragsstammdaten von Mitarbeitern
7. Mitarbeiterhistorie
8. Vertragsabrechnungs- und Zahlungsdaten von Mitarbeitern und ggfls. Bewerbern
9. Auskunftsangaben von Dritten zu einem Bewerber
10. Gerichtliche oder außergerichtliche Verfahrensdaten (z.B. Abmahnungen) von Mitarbeitern
11. Daten der Zeiterfassung und der Gebäudezugangskontrolle von Mitarbeitern
12. Unterlagen zu Reisen von Mitarbeitern und ggfls. von Bewerbern
13. Bewerbungsunterlagen (inkl. Bilder) und Zeugnisse von Mitarbeitern und Bewerbern
14. Daten von Mitarbeitern, die zum Betrieb der Software im Rechenzentrum nötig sind.
15. Sonstige Arten von personenbezogenen Daten (z.B. Bruttolohndatei)

Die Entscheidung, welche Arten von personenbezogenen Daten von Mitarbeitern bzw. Bewerbern mit den o.g. IT-Produkten zusätzlich zu den genannten Datenkategorien verarbeitet werden obliegt gemäß § 4 (2) der Vereinbarung zur Auftragsverarbeitung dem Verantwortlichen.

** Subunternehmen, Standort der Datenverarbeitung und erbrachte Teilleistungen

A) Sage People
- Sage People Ltd., Reading, UK, Bereitstellung und Betrieb der Software, Unterstützung bei Supportanfragen oder Remote-Support, Professional Services Leistungen
- Sales Force Inc., San Francisco, CA, USA, Rechenzentrum Frankfurt a.M., System-Administration von Servern und Services, ISO 27001-Zertifikat: https://compliance.salesforce.com/en/iso-27001

B) Sage People Recruiting
Sovren Inc., Marble Falls, Texas, USA, Bereitstellung und Betrieb einer OCR-Software für Bewerbungen

Technische und organisatorische Maßnahmen (Anhang TOM) i.S.d. Art. 32 DSGVO
Sage GmbH, Frankfurt a.M.
Stand: 19.7.2021

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO)

1.1 Zutrittskontrolle

Der allgemeine Zutritt zum Gebäude erfolgt über ein elektronisches Zutrittskontrollsystem. Besucher müssen sich am Empfang anmelden, Ihre Identität wird überprüft und sie dürfen nur in Begleitung eines Sage Mitarbeiters die Räumlichkeiten betreten.

Der Zutritt zum Serverraum wird über ein elektronisches Zutrittskontrollsystem kontrolliert. Zugang haben nur ausgewählte Mitarbeiter der IT.

Alle Räumlichkeiten sind außerhalb der Arbeitszeiten mittels Alarmanlage gesichert. Alarmbereitschaft eines Wachschutzes ist gegeben.

1.2 Zugangskontrolle

Für die Anmeldung an das Netzwerk ist ein Kennwort mit einer vorgegebenen Mindestlänge erforderlich. Dabei sind Zahlen und Sonderzeichen zu verwenden sowie Groß- und Kleinschreibung zu beachten. Für Zugriffe außerhalb des VPN wird eine 2-Faktor-Authentifizierung verlangt.

Eine automatische Sperrung des Benutzers erfolgt nach drei falschen Eingaben bei der Benutzeranmeldung. Das Kennwort ist spätestens nach 90 Tagen zu ändern. Die Aufforderung dazu erfolgt automatisch. Eine Aktivierung des Bildschirmschoners erfolgt nach 10 Minuten und kann nur wieder über Passworteingabe freigegeben werden.

Die Benutzerauthentifizierung wird mittels eines zentralen Verzeichnisdienstes abgebildet. Grundsätzlich und soweit nicht technisch notwendig, ist ein Zugang zu Auftragsdaten nur mittels personifizierten Accounts zugelassen.

Das System wird durch eine Firewall ständig überwacht. Es gibt eine Antivirus-Software auf Systemebene. Darüber hinaus ist für das Mail-System eine Antivirus-Software je Client sowie Server installiert. Es werden ausschließlich IT-Systeme eingesetzt, die vom Hersteller durch regelmäßige Sicherheitsupdates unterstützt werden.

1.3 Zugriffskontrolle

Die Zugriffskontrolle ist in differenzierten Berechtigungen auf Menü-Ebene eingerichtet. Ein elektronischer Datensafe überwacht den Zugang der Supportmitarbeiter zu Kundendaten. Zugriffe auf Anwendungen werden protokolliert.

1.4 Trennungskontrolle

Soweit eine getrennte Verarbeitung von Datenbeständen erforderlich ist, wurde diese entsprechend eingerichtet. Für Tests oder Entwicklung gibt es eigene Domains.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO; Art. 25 Abs. 1 DSGVO)

Datenbanken der Sage Produkte und unserer internen IT-Systeme sind normalisiert – soweit Business Prozesse es nicht anders erfordern. Das heißt, personenbezogene Daten werden für gewöhnlich in eigenen Datenbanktabellen gespeichert. Sie sind mit Verarbeitungsvorgängen, wie z.B. Tickets, Abrechnungen, Dokumente etc. über Schlüssel verknüpft. Passwörter werden verschlüsselt gespeichert.

2. Integrität (Art. 32 Abs. 1 lit. B DSGVO)

2.1 Weitergabekontrolle

Der Transport außerhalb des jeweiligen Netzwerks erfolgt verschlüsselt. Hierzu werden starke Verschlüsselungsalgorithmen eingesetzt. Kundendaten können nur elektronisch direkt in den Datensafe übermittelt werden. Personenbezogene Daten aus dem Datensafe werden nicht weitergegeben. Sie werden mit Abschluss eines Supporttickets automatisch nach einer Frist von 4 Wochen gelöscht.

Alle gemäß §§ 15 ff. AktG verbundenen Unternehmen in Zentraleuropa sind über eine Standleitung zwischen den Standorten verbunden.

2.2 Eingabekontrolle

Alle Netzwerkan- und -abmeldungen sowie sämtliche Transaktionen (z.B. Neuanlagen, Veränderungen, Löschungen) werden protokolliert. Die Protokolle werden hinsichtlich unberechtigter Zugriffe analysiert und nach 6 Monaten gelöscht.

Spezielle Werkzeuge überwachen außerdem unseren gesamten internen und externen Netzwerkverkehr auf ungewöhnliche Aktivitäten und melden diese automatisch, um weitere Nachforschungen anzustoßen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DSGVO)

3.1 Verfügbarkeitskontrolle

Es wird ein wöchentliches Backup (Vollsicherung) durchgeführt. Dazu wird zusätzlich täglich inkrementell gesichert. Die Sicherung erfolgt in zwei räumlich getrennten Rechenzentrums-Bereichen auf entsprechenden Storage Systemen.

Es wird ein RAID-Verfahren bei den Festplattensicherungen eingesetzt. Unterbrechungsfreie Stromversorgung (USV) samt Überspannungsschutz ist vorhanden.

Durch den Einsatz der Firewall und der Antivirus-Software für das Mail-System und alle Server, sowie Antivirus-Software je Client wird die Verfügbarkeit technisch bestmöglich sichergestellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO, Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Alle Mitarbeiter bei Sage sind auf das Datengeheimnis verpflichtet. Es erfolgt eine regelmäßige Unterweisung der Mitarbeiter im Datenschutz. Ein Datenschutzkonzept und eine IT-Policy wurden erstellt. Zusätzlich existieren Sage-weit geltende Richtlinien zur Informationssicherheit und zum Schutz personenbezogener Daten. OneTrust dient als konzernweite Software-Lösung für das Management des Datenschutzes.

Ein Datenschutzbeauftragter wurde bestellt: Achim Hubert, E-Mail: datenschutzbeauftragter@sage.com. Die Organisation kommt ihren Informationspflichten nach Art. 13 und 14 DSGVO nach. Für die Bearbeitung von Auskunftsanfragen seitens Betroffener existiert ein formalisierter Prozess. Für die eingesetzten IT-Systeme und Prozesse existieren Verarbeitungsverzeichnisse. Die Wirksamkeit unserer technischen und organisatorischen Schutzmaßnahmen wird in Abstimmung mit dem Sage-Konzern regelmäßig überprüft.

4.2 Incident-Response-Management

Firewalls, Spamfilter und Virenscanner werden eingesetzt und regelmäßig aktualisiert. Daneben existieren Systeme zur „Intrusion Detection and Prevention“. Eine Policy regelt den Umgang mit Sicherheitsvorfällen. Es gibt Alarmpläne und eine Dokumentation von Sicherheitsvorfällen und Datenpannen. Dabei werden der Datenschutzbeauftragte, der Security Officer sowie die Rechtsabteilung stets involviert. In Abstimmung mit dem Datenschutzbeauftragten erfolgen Meldungen gegenüber den Aufsichtsbehörden.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die Prozesse für Softwarepflegeleistungen, die im Zusammenhang mit personenbezogenen Daten stehen, sind klar definiert und die involvierten Mitarbeiter sind per bindender Arbeitsanweisung entsprechend verpflichtet. Dazu gehört, dass Kundendaten nur über den Datensafe entgegengenommen und verwaltet werden. Die Mitarbeiter sind angehalten nicht mehr personenbezogene Daten zu erheben, als für den jeweiligen Zweck erforderlich sind. Aufzeichnungen von Remote-Sitzungen werden nach 4 Wochen automatisch gelöscht.

4.4 Auftragskontrolle (Outsourcing an Dritte)

Unsere Mitarbeiter kennen den Datenverarbeitungszweck. Sie erhalten Weisungen zum Umgang mit personenbezogenen Daten. Spezielle Unterauftragsverhältnisse (Subunternehmer) werden schriftlich beauftragt und sind bei den jeweiligen Produkten bzw. Services im Anhang Produkte zur AV-Vereinbarung aufgeführt. Zwischen den einzelnen Sage-Gesellschaften bestehen Vereinbarungen zur Auftragsverarbeitung (C2C und C2P) auf Basis von EU-Standardvertragsklauseln.