Vereinbarung
über die Verarbeitung personenbezogener Daten
(Auftragsverarbeitung)

zwischen

Name: . . . . . .
Straße: . . . . . .
PLZ Ort: . . . . . .

- nachstehend Auftraggeber genannt -

und

Funk, Zander & Partner Gesellschaft für EDV-Beratung und
anwenderbezogene Schulungen mbH
Torgauer Straße 231
04347 Leipzig

- 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, ab dem 25.05.2018 aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) sowie der nationalen Datenschutzgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet (Anlage 1). Sie findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag/Hauptverträgen (im Einzelnen in Anlage 1 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 Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/ Backup-Datei – vor allem im Zusammenhang mit Supportanfragen – 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 der Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf mit dem Laufzeitende des letzten verbleibenden, in Anlage 1 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 Supportangebote weitergehende Hilfestellungen im Umgang mit der Software an. Ferner bietet er Softwarelösungen 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 Hauptvertrages konkretisiert. Die Hauptverträge sind ferner in Anhang 1 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 verantwortliche Stelle 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. Der Auftragnehmer dokumentiert alle Weisungen des Auftraggebers, unabhängig davon in welcher Form diese ergangen sind. 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.

Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen

(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 dieser technischen und organisatorischen Maßnahmen wird als Anlage 2 diesem Vertrag beigefügt.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

(4) Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit. Anlage 4

(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 (Pflichten aus Kapitel III und den Art. 32 bis 36 DSGVO), 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). Der Auftraggeber erstattet dem Auftragnehmer durch die Unterstützung entstehende Kosten und Aufwand. Können sich die Parteien nicht über den Umfang der Erstattung einigen, werden die Kosten, die der Auftragnehmer für erforderlich halten durfte, in vollem Umfang erstattet.

(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 auf Verlangen in geeigneter Weise nachzuweisen.

(8) Die Auftragsverarbeitung darf nur innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Eine Verlagerung in ein Drittland außerhalb dieses Gebietes bedarf der vorherigen Zustimmung des Auftraggebers.

(9) Der Auftragnehmer verpflichtet alle Mitarbeiter, die zur Verarbeitung personenbezogener Daten befugt sind, vor Beginn der Verarbeitungstätigkeiten zur Verschwiegenheit, soweit dieser nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 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 Auftraggeber trägt hierdurch anfallende Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.

(3) Der Auftraggeber ist als Verantwortlicher 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 auf erstes Anfordern freistellen. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt (insbesondere hinsichtlich Berichtigung, Löschung und Sperrung von Daten), erstattet der Auftraggeber dem Auftragnehmer Kosten und Aufwand. Die Parteien verständigen sich über den erwarteten Umfang von Kosten und Aufwand.

(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 Kontrollpflichten

(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 beiliegender Anlage 2 zu überzeugen.

§ 6 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen die in der Anlage 3 benannten weiteren Auftragsverarbeiter (Subunternehmer) einschaltet. Über eine Änderung der in der Anlage 3 genannten Subunternehmer wird der Auftragnehmer den Auftraggeber informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Im Übrigen ist die Beauftragung von Subunternehmern durch den Auftragnehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nur aus wichtigem, dem Auftragnehmer nachzuweisendem Grund verweigert werden. 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.

§ 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 „verantwortlicher Stelle“ im Sinne des anwendbaren Datenschutzrechts liegen.

§ 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. Dadurch resultierende zusätzliche Kosten durch die Herausgabe oder Löschung der Daten sind vom Auftraggeber zu tragen.

§ 9 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Weisungsberechtigte Personen des Auftraggebers sind: (bitte max. 2 Personen je Geschäftseinheit angeben)

(Name, Organisationseinheit, Funktion, Telefon, E-Mail)

(2) Weisungsempfänger beim Aufragnehmer sind:

Supportabteilung Funk, Zander & Partner GmbH
Tel.: +49 341 2259922
Fax: +49 341 2259933
E-Mail: support@fzp-beratung.com

Der im Auftrag festgelegte Projektleiter.

§ 10 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.

(2) Änderungen und Ergänzungen dieser Anlage 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) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Ausschließlicher Gerichtsstand ist Leipzig.

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

Ort, Datum _____ Ort, Datum _____

_____ _____
Auftraggeber Auftragnehmer

Anlage 1
Umfang, Art und Zweck der Datenverarbeitung

I. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien: (bitte zutreffendes ankreuzen)

Hauptvertrag	Betroffen Datenkategorien *
☐ Sage ERP	1,2,3,4,5,6,7,8
☐ CRM	1,2,3,8
☐ DMS	1,2,3,4,5,6
☐ FZP-Module	Nur in Verbindung mit einem Sage Modul
☐ Sage HR	9,10,11,12,13,14

* Datenkategorien und Personen:

1. Kontaktdaten und -historie bzgl. natürlicher Personen d.h. Kunden, Lieferanten, Ansprechpartner von Firmen, Interessenten und Vertretern
2. Daten zur Geschäftshistorie von Kunden, Lieferanten und Vertretern
3. Daten von Mitarbeitern bzw. Anwendern des Systems
4. Daten zu finanziellen Transaktionen von Kunden, Lieferanten und Vertretern
5. Daten zu Bankverbindungen und Zahlungsarten von Kunden, Lieferanten und Vertretern
6. Daten zur Vermögens- und Ertragssituation von Kunden und Lieferanten
7. Daten zu Arbeitszeiten und Abläufen von Mitarbeiter (nur bei Einsatz Sage Aufgaben-Center und Webclient)
8. Sonstige (unstrukturierte) personenbezogene Daten von Kunden, Lieferanten, Ansprechpartnern von Firmen, Interessenten, Vertretern, Mitarbeitern und Anwendern des Systems
9. Alle personen- und unternehmensbezogenen Daten, die zur Abrechnung der Mitarbeiter nötig sind und zur Meldung an z.B. Finanzamt und Krankenkasse benötigt werden (Personalabrechnung)
10. Alle Daten, die zur Verwaltung und Planung der Mitarbeiter im Unternehmen erhoben werden (Personalmanagement)
11. Alle Daten, die ein Bewerber zum Bewerbungszweck eingibt oder der Bewerbung beifügt. Dies umfasst auch Bilder und Kopien von Dokumenten (Bewerbermanagement)
12. Alle Daten der Zugangskontrolle, An-und Ab-wesenheiten der Mitarbeiter (Zeitmanagement)
13. Alle Daten, die den Mitarbeiter im Unternehmen bezogen auf Weiterbildung, Urlaub-und Fehlzeiten sowie Reisen betreffen (Mitarbeiterportal)
14. Alle Daten, die zur Beantragung, Genehmigung und Abrechnung von Reisen benötigt werden (Reisemanagement)

Soweit eines der o.g. Produkte nicht den Funktionsumfang aufweist, entfallen die Datenkategorien für einige der genannten Personen. Gleichzeitig ist es aber auch in einigen Produkten möglich, individuell die Datenkategorien zu erweitern oder anders als vorgesehen zu nutzen. Dies obliegt gemäß § 4 (2) der Vereinbarung zur Auftragsverarbeitung dem Anwender der Produkte.

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 Anwender unserer Produkte

II. Kreis der Betroffenen

Die übertragenen personenbezogenen Daten betreffen die folgenden Personengruppen: (Bitte nicht zutreffendes durchstreichen bzw. gegebenenfalls erweitern)

Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Handelsvertreter, Ansprechpartner, Vertreter, Mitarbeiter……

……

……

III. Gegenstand und Zweck der Datenverarbeitung

Der Gegenstand des Auftrags ergibt sich aus allen gültigen Softwarepflegeverträgen sowie in den Konzepten, Angeboten, Aufträgen und sonstigen Verträgen (z.B. Werksverträge, Dienstleistungsverträge/Kontingente, Rahmenverträge, u.ä.) beschriebenen Leistungen.

In der Regel sind dies:

Einführung, Installation, Wartung, Support (Fernwartung) und Betreuung der Sage-Software sowie der FZP-Module.

Anlage 2
Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, konkretisiert diese Anlage nach Artikel 32 EU-Datenschutzgrundverordnung („DSGVO"), die getroffenen technischen und organisatorischen Schutzmaßnahmen, die sich aus der Rahmendatenschutzvereinbarung zur Sicherstellung der Konformität zum Artikel 28 EU Datenschutz-Grundverordnung (DSGVO) für die Verarbeitung personenbezogener Daten im Auftrag in Verbindung mit den jeweiligen projektbezogenen Ergänzungen in seinen Einzelheiten beschriebenen Datenverarbeitung ergeben, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.

Nr.	Prüfungspunkt	Antwort
0.	Organisationskontrolle	
0.1	Wie ist die Umsetzung des Datenschutzes organisiert? (interner/externer Datenschutzbeauftragter, freiwillige Bestellung ohne gesetzlichen Zwang, hauptamtliche/nebenamtliche Bestellung, Datenschutzorganisation etc.) *[Vorgaben aus Artikel 30, 37 DSGVO, ISO 27001]*	Benennung / Bestellung eines externen Datenschutzbeauftragten, nebenamtlicher interner Mitarbeiter zur Abstimmung und Koordination aller datenschutzrechtlichen Angelegenheiten.
0.2	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt? (Verpflichtung der Mitarbeiter zur Vertraulichkeit, Datenschutzordnung, interne Arbeitsanweisungen etc.) *[Vorgaben aus Artikel 28 Abs. 3 Satz 2 lit. b) DSGVO, ggf. § 88 TKG]*	Verpflichtung aller Mitarbeiter auf das Datengeheimnis / die datenschutzrechtliche Vertraulichkeit, Aufstellung von Richtlinien mit datenschutzrechtlichem Bezug
0.3	Wie wird sichergestellt, dass die internen Prozesse bzw. Arbeitsabläufe gemäß der jeweils aktuell gültigen Datenschutzbestimmungen ablaufen und wird dies regelmäßig einer Qualitätsprüfung unterzogen? (Auditierung der internen Prozesse, Schulung der Mitarbeiter etc.) *[Vorgaben aus Artikel 39, ISO 27001]*	Auditierung durch externen Datenschutzbeauftragten, jährliche Schulung und Sensibilisierung der Mitarbeiter, datenschutzrechtliche Verpflichtung und Belehrung
0.4	In welcher Form werden die Mitarbeiter in Bezug auf die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO geschult? (Einweisungen, Präsenzschulungen, Arbeitsanweisungen etc.) *[Vorgabe ISO 27001]*	Präsenzschulung in den Räumen des Auftragsverarbeiters, Aufstellung von Richtlinien mit datenschutzrechtlichem Bezug, externe Mitarbeiterschulungen
0.5	Wie sind die einschlägigen Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit (z.B. Datenschutz-Folgeabschätzung) dokumentiert? (Verzeichnis von Verarbeitungstätigkeiten, Dokumentation Datenschutz-Folgeabschätzung etc.) *[Vorgabe aus Artikel 30, 35 DSGVO]*	Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten als Verantwortlicher und Auftragsverarbeiter, Einbeziehung des Datenschutzbeauftragten bei der Dokumentation / Beurteilung von Datenverarbeitungen

Nr.	Prüfungspunkt	Antwort
0.6	Welche Vorkehrungen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen werden getroffen? (Überprüfung des Datenschutz- oder Sicherheitskonzept durch Penetrationstest und sonstige simulierte Angriffe, regelmäßige Auditierungen) *[Vorgabe aus Artikel 32 Abs. 1 lit. d DSGVO]*	Externe Auditierung durch Datenschutzbeauftragten, Analyse / Prüfung von verdächtigen Aktivitäten
1.	Maßnahmen zur Zutrittskontrolle	
1.1	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? (Schließverfahren, elektronische Zutrittskontrolle, Videoüberwachung, Einbruchssicherung, Wachpersonal, Alarmanlage, Bewegungsmelder etc.) [Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO]	Bürogebäude durch Wachschutz abgesichert, elektrischer Türschließer, Transpondersystem, Sicherheitsschlösser, Schließregelungen für Bürogebäude, Büros und Tor, Absicherung des Serverraums mit Zutrittsregelung, Regelung zur Schlüsselvergabe, Videoüberwachung, ständig besetzter Empfang während der Geschäftszeiten
1.2	Wie werden die Räume/Büros, in denen die personenbezogenen Daten verarbeitet werden, vor unbefugtem Zutritt gesichert? (Schließverfahren, elektronische Zutrittskontrolle, Alarmanlage, Rollläden mit Hochschiebesicherung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO]*	Abschließbare Büros, Schließregelungen, Regelungen zur Schlüsselvergabe, elektrischer Tierschließer
1.3	Wie werden die Hardwarekomponenten selbst vor Missbrauch geschützt? (Diebstahlschutz z.B. durch Kensington-Lock für Notebooks, PC-Schutzschrank, Wegschließen nach Arbeitsende etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO]*	Hardwarekomponenten werden außerhalb der Betriebszeiten unter Verschluss gehalten, gesonderte Absicherung der Serverräume, Zutritt nur durch autorisierte Personen, Überwachung des Bürogebäudes durch Wachdienst und Videoüberwachung
1.4	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft? (Dokumentierte Testverfahren etc.) *[Vorgabe ISO 27001]*	regelmäßige Prüfung der Richtlinien / Regelungen wie kontrollierte dokumentierte Schlüsselvergabe.
1.	Maßnahmen zur Zugangskontrolle	
2.1	Benutzerverwaltung	
2.1.1	Wie erfolgt die Vergabe von Benutzerzugängen (-accounts)? (Standardisierter Prozess zur Antragstellung, Genehmigung, Einrichtung, Änderung, Löschung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Die Berechtigungen werden rollenbasiert entsprechend der Aufgabe des Mitarbeiters als individuelle, dokumentierte Berechtigung vergeben. Die Freigabe erfolgt durch die Geschäftsführung und den Systemadministrator. Die Systeme sind mehrstufig mit Passwort geschützt. 1. Clientzugang 2. Serverzugang 3. Zugang zur Anwendung Berechtigung zum Zugriff auf Datenbanken haben nur autorisierte Personen.

Nr.	Prüfungspunkt	Antwort
2.1.2	Wie wird die Gültigkeit von Benutzerzugängen (-accounts) überprüft? (bei geänderter Aufgabenstellung, Versetzungen, Austritten; regelmäßige Prüfung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Unmittelbar mit Änderungen der Aufgabenstellung / Austritt / Versetzung erfolgt eine Anpassung bzw. Löschung der Berechtigungen bzw. Benutzerzugänge, Dokumentation im Rahmen der Netzwerkdokumentation, regelmäßige Prüfung, zusätzlich vorgegebenes Ablauf-/Deaktivierungsdatum
2.1.3	Wie werden Benutzerzugänge (-accounts) (inkl. Antrags- und Genehmigungsverfahren, Änderungsverfahren) dokumentiert? (Systemprotokollierung, Workflow-Management etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Schriftliche Dokumentation im Rahmen der Netzwerkdokumentation, schriftliche Dokumentation / Weisungen je nach Berechtigtem
2.1.4	Wie stellen Sie sicher, dass a) die Vergabe von Administrationszugängen auf die notwendige Anzahl beschränkt ist? b) diese Administratoren die fachlich und persönlich geeignet sind? c) externe Administratoren, Service oder Wartungstechniker persönlich geeignet sind? *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Beschränkung der Administrationsrechte auf ein Minimum Berechtigter. Notfallpasswörter werden in einem versiegelten Umschlag in einer verschlossenen Kasse in einem speziell gesicherten Stahlschrank verwahrt. Der Systemadministrator ist speziell geschult und ein langjähriger Mitarbeiter. Zugänge / Änderungen von Berechtigungen werden nur auf Anweisung durch die Geschäftsführung freigegeben und individuell dokumentiert.
2.2	Passwortsicherheit	
2.2.1	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind und keinem Unbefugten? (Verschlüsselte Speicherung, sichere Übermittlung, Verbot der Weitergabe von Passwörtern, Anweisung zur Geheimhaltung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Verbindliches Verfahren zur Rücksetzung von Passwörtern durch IT-Administration, Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passwörtern, Vorgabe zur regelmäßigen Änderungen aller Passwörter mit Pflichtvorgaben: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Mindestlänge von Passwörtern beträgt 8 Zeichen, Mindestlänge für administrative Passwörter beträgt 12 Zeichen
2.2.2	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt? (Mindestlänge, Aufbau, Historie, Vermeidung von Trivialpasswörtern etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Vorgabe zur regelmäßigen Änderungen aller Passwörter (90 Tage) mit Pflichtvorgaben: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Mindestlänge von Passwörtern beträgt 8 Zeichen, Mindestlänge für administrative Passwörter beträgt 12 Zeichen
2.2.3	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann bzw. muss? (Erzwungener Passwortwechsel bei Erstanmeldung bzw. in regelmäßigen Abständen, jederzeitige Möglichkeit des Benutzers, das Passwort zu ändern) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Erzwungener Passwortwechsel bei Erstanmeldung, eine Passwortänderung ist technisch alle 90 Tage vorgegeben, die Vergabe gleicher Passwörter ist technisch ausgeschlossen

Nr.	Prüfungspunkt	Antwort
2.2.4	Wie erfolgt die Administration von Passwörtern? (Standardisierter Prozess zur Passwort-Vergabe, Rücksetzung von gesperrten Benutzerkonten, sichere Authentifizierung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Passwörter der Anwendungen (ERP- und HR-System) sind über die Windows-Anmeldung gesteuert (Domäne) und gesichert. Änderung der Windows-Passworte wird alle 90 Tage erzwungen. Administration der Domäne erfolgt über den Administrator, vorgegebener Prozess zur Passwortänderung
2.2.5	Welche Maßnahmen werden bei gescheiterten Anmeldeversuchen zur Abwehr unberechtigter Zugriffe ergriffen? (Art und Weise der Sperrung des Benutzerkontos (z.B. nach n-Fehlversuchen, temporäre Sperrung), automatische Information an Systemadministrator etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Protokollierung durch Logfiles. Bei (mutmaßlichen) Angriffen automatisierte Meldungen an den Administrator, Sperrung der Zugriffe und Einleitung erforderlicher Maßnahmen.
2.2.6	Welche organisatorischen Vorkehrungen werden zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz getroffen? (regelmäßige Unterweisungen zum Umgang mit PCs, Kopierern und Fax-Geräten, Handhabung von Dokumenten etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugangskontrolle]*	Regelmäßige technische und datenschutzrechtliche Unterweisung / Belehrung von Mitarbeitern, Sensibilisierung, Vorgabe zur zeitgesteuerten Sperrung aller Arbeitsplätze / Eingabegeräte
3.	Maßnahmen zur Zugriffskontrolle	
3.1	Wie wird sichergestellt, dass Rollen / Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden? (Standardisierter Vergabeprozess, 4-Augen-Prinzip, Genehmigung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugriffskontrolle]*	Standardisierte Vergabeprozesse mit vorgegebenem 4-Augen-Prinzip, Standardisierter Vergabeprozess mit verpflichtender Genehmigung durch die Geschäftsführung, regelmäßige Kontrolle durch die Geschäftsführung, automatisierte Deaktivierung (nach 5 Fehlversuchen, Neue Mitarbeiter nach 6 Monaten, Mitarbeiter nach einem Jahr)
3.2	Wie erfolgt die Dokumentation der Zugriffsberechtigungen? (Berechtigungskonzept, Rollenvergabe, Anträge etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugriffskontrolle]*	Dokumentation der Berechtigungen und Rollenvergaben im Rahmen einer Netzwerkdokumentation / individuellen berechtigungsbezogenen Dokumentation
3.3	Wie wird sichergestellt, dass Benutzer ihre Zugriffsberechtigung nicht missbräuchlich verwenden? (Monitoring, Protokollierung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Zugriffskontrolle]*	Dokumentation und Protokollierung der Zugänge, Kontrolle / Monitoring der Zugriffe
4.	Maßnahmen zur Weitergabekontrolle	
4.1	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten? (vertragliche Abreden, technische Maßnahmen (z.B. elektronische Signaturen, Verschlüsselungen) etc.)	Belehrung und Sensibilisierung der Mitarbeiter, Freigabe / Weisung als Voraussetzung, VPN-Verschlüsselung, verschlüsselte Datenübertragung, E-Mail-Verschlüsselung

	[Schutz der Vertraulichkeit und Integrität nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]	
Nr.	Prüfungspunkt	Antwort
4.2	Welche Verschlüsselungssysteme werden bei der Weitergabe von personenbezogenen Daten eingesetzt? (Ipsec-Verfahren, SSH-Verfahren, verschlüsselte Plattformen zum Datenaustausch, E-Mail-Verschlüsselung etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. a und b DS-GVO, ISO 27001]*	Passwortversand über verschlüsselte E-Mails, separate Verschlüsselung von Daten mit höchstmöglicher Verschlüsselung, getrennte Übermittlung von sensiblen Informationen
4.3	Wie wird die Weitergabe personenbezogener Daten dokumentiert? (Konzept zur Weitergabe von Daten, Protokollierung von Datenabrufen, Empfängerliste etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Dokumentation im internen PM-System, unmittelbare Kommunikation, Festlegung / Dokumentation von Empfängerlisten
4.4	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt? (Berechtigungen für Download, Ausdruck, Speichern beschränken etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Beschränkte Berechtigungen nur für jeweils autorisiertes Personal soweit zwingend erforderlich, individuelle Zugriffsbeschränkung
4.5	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann? (Systemseitige Protokollierung und regelmäßiger Auswerteprozess etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Systemseitige Dokumentation / Zugriffsprotokollierung, Auswertung von Logfiles
5.	Maßnahmen zur Eingabekontrolle	
5.1	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf die Applikationen zugegriffen hat? (Login-, Logout-Protokollierung etc.) *[Schutz der Vertraulichkeit und Integrität nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Korrekte Verarbeitung in Anwendungen]*	Dauerhaftes Reporting der Firewall an IT-Administration, bei potentiellen Angriffen / nicht authentifizierten Zugriffen automatisierte Meldungen und Prüfung. Protokollierung / Log von Log-out, Log-in, Protokollierung / Analyse von verdächtigen Eingaben
5.2	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden? (Protokollierung von Eingabe, Änderungs- bzw. Löschzugriffen, Starten von Reports etc.) *[Schutz der Vertraulichkeit und Integrität nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001-Korrekte Verarbeitung in Anwendungen]*	Alle Änderungen an Daten in der Software SAGE werden mittels Protokollierungssystemen protokolliert. Die Software SAGE als GoB- und ITSG-zertifiziertes System umfasst diese Funktionen je nach individueller Konfiguration als Standard.
6.	Maßnahmen zur Auftragskontrolle	
6.1	Welche Maßnahmen werden ergriffen, damit die Verarbeitung der personenbezogenen Daten durch die damit betrauten Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann? (Richtlinien, Arbeitsanweisungen, Zugriffssteuerung, Verpflichtung auf das Datengeheimnis etc.) *[Schutz der Vertraulichkeit, Integrität und Verfügbarkeit nach Artikel 32 Abs. 1 lit. b DS-GVO]*	Vertragliche Absicherung / datenschutzrechtliche Verpflichtung, Auswahl nach Sorgfaltsgesichtspunkten, Unternehmensrichtlinien, Arbeits- und Organisationsanweisungen und Verpflichtung im Arbeitsvertrag sowie regelmäßige schriftliche Belehrungen und Schulungen.

Nr.	Prüfungspunkt	Antwort
6.2	Welche Maßnahmen werden getroffen, damit auch ggf. Unterauftragnehmer keine unbefugten Aktivitäten mit den zur Verfügung gestellten Daten durchführt? (sorgfältige Auswahl der Unterauftragnehmer, vertragliche Verpflichtung der Unterauftragnehmer etc.) *[Schutz der Vertraulichkeit, Integrität und Verfügbarkeit nach Artikel 32 Abs. 1 lit. b DS-GVO]*	Auswahl der Unterauftragnehmer nach Sorgfaltsgesichtspunkten, vertragliche Verpflichtung, eindeutige Vertragsgestaltung
6.3	Werden Maßnahmen getroffen, die am Ende des Aufbewahrungszwecks der personenbezogenen Daten deren Löschung/ Sperrung sicherstellen und sind diese technisch implementiert? (sorgfältige Auswahl der Unterauftragnehmer, vertragliche Verpflichtung der Unterauftragnehmer etc.) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO]*	Die Daten werden unmittelbar nach Wegfall des Zwecks / auf Weisung vom FTP-Server gelöscht. Kundendatenbanken werden auf einem jeweils separaten Serverlaufwerk gespeichert, Einbindung in virtuelle Entwicklungsumgebung auf dem Server oder lokal zu Testzwecken, für Datenmigrationen, Fehleranalysen u. Ä. eingebunden. Wenn die Arbeiten abgeschlossen sind, werden die Daten und die Datenträger sicher / nicht wiederherstellbar gelöscht und / oder zerstört (z. B. Schreddern von DVDs).
7.	Maßnahmen zur Verfügbarkeits- und Belastbarkeitskontrolle	
7.1	Werden organisatorische und technische Maßnahmen getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellst möglichst zu gewährleisten? (Backup und Disaster-Recovery mit Notfallplänen, Spiegeln von Festplatten an getrennten Data-Center-Lokationen mit adäquaten Betriebsszenarien (unabhängige Stromversorgung) etc.) *[Schutz der Verfügbarkeit und Belastbarkeit der System nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Einsatz eines redundanten Serversystems mit separatem Datensicherheitskonzept. Komplette Neukonzeption und Anschaffung 2015, Back-up-Konzept
7.2	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlungen etc.) geschützt sind? (Rauch- & Brandmelder, Sprinkleranlage, Brandschutztüren, Wasserschutzeinrichtungen, Schirmdämpfung etc.) *[Schutz der Verfügbarkeit und Belastbarkeit der Systeme nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Brandschutztür zu den Büroräumen. Brandmelder und Feuerlöscher in den Büroräumen. Nächtliche Überwachung durch Sicherheitsdienst sowie Überwachung der Feuerwehrzufahrten. Keine Heizung im Serverraum. Elektromagnetischer Schutz wird durch geschlossenen Raum und zusätzlich durch gesondert gesicherten Serverschrank gewährleistet, Unterbrechungsfreie Stromversorgung
7.3	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet? (Virenscanner, Firewalls, Anti-Spy-Programme, Spam-Filter, IDS-/IPS-Systeme, Vorgehensweise zur Aktualisierung etc.) *[Schutz der Vertraulichkeit, Integrität und Verfügbarkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Virenscanner, Firewalls, Anti-Spy-Programme, Spam-Filter mit aktiven Wartungsverträgen. Dauerhafte Überwachung erfolgt durch den Systemadministrator und Stellvertreter
7.4	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden? (Beauftragung von speziellen Entsorgungsunternehmen und deren Überprüfung etc) *[Schutz der Vertraulichkeit nach Artikel 32 Abs. 1 lit. b DS-GVO, ISO 27001]*	Spezielle externe Entsorgung / spezieller Schredder / Vernichtungsgeräte (Auf dem Übergabeprotokoll wird die „Verschrottung“ dokumentiert. Keine Lagerung. Die Behältnisse (z.B. Entsorgungsbox für Datenträger) stehen bei uns und werden entsorgt, sobald sie voll sind.)

Nr.	Prüfungspunkt	Antwort
7.5	Welche Maßnahmen werden zur Sicherstellung der Belastbarkeit der Systeme und Dienste und zur Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall getroffen? (Redundanz der Systeme, Schutz gegen DDoS-Angriffe, rasche Wiederherstellbarkeit, Übungen und Tests zur Wiederherstellung) *Vorgaben aus Artikel 32 Abs. 1 lit. b und c DSGVO]*	RAID-Systeme, Back-up-Konzept, räumlich getrennte Sicherungen, parallele / redundante Sicherheitssysteme, Schutz gegen DDoS-Angriffe, Übungen und Tests für rasche Wiederherstellbarkeit
8.	Maßnahmen zur Trennungskontrolle	
8.1	Welche Maßnahmen werden getroffen, um das Trennungsgebot, insbesondere in Bezug auf die Zweckgebundenheit der personenbezogenen Daten, zu gewährleisten? *(*Nutzung von unterschiedlichen, kundenspezifischen bzw. mandantenfähigen Systemen, detaillierte Zugriffskonzepte, Verschlüsselung der Datensätze etc.) *[Schutz der Vertraulichkeit und Integrität nach Artikel 32 Abs. 1 lit. b DS-GVO]*	Separate Serverlaufwerke für Kundendaten, virtuelle Maschinen, Trennung von Test- und Produktivsystemen, Zugriffsberechtigung, verschlüsselte Speicherung, Verschlüsselung von virtuellen Systemen
9.	Maßnahmen zur Pseudonymisierung und Anonymisierung	
	Welche Maßnahmen werden zur Pseudonymisierung und Anonymisierung personenbezogener Daten getroffen? (Pseudonymisierung ist die Verarbeitung personenbezogene Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Existieren solche zusätzlichen Informationen nicht oder werden sie unwiderruflich gelöscht, so handelt es sich um eine Anonymisierung.) *[Vorgaben aus Artikel 32 Abs. 1 lit. a DSGVO]*	Kommt für Softwarepflegeleistungen nicht als Option in Betracht. Personenbezogene Daten aus dem Datensafe werden nicht weitergegeben. Fristgerechte Löschung von Daten.

Anlage 3
Weitere Auftragsverarbeiter

Gemäß § 6.1 stimmt der Auftraggeber mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgende weitere Auftragsverarbeiter im Rahmen der Datenverarbeitungstätigkeiten einsetzt:

Weiterer Auftragsverarbeiter (Subunternehmer)	Sage GmbH
Adresse	Franklinstraße 61 - 63 60486 Frankfurt/Main
Telefonnummer; E-Mail	069/50007-0; info@sage.de
Ansprechpartner	Geschäftsführer: Heino Erdmann
Der weitere Auftragsverarbeiter unterstützt in folgenden Datenverarbeitungstätigkeiten	3rd Level Support für das in Anlage 1 genannte Produkt. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/Backup, 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.

Anlage 4
Datenschutzbeauftragter

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 28 und 29 DS-GVO ausübt.

Als externer Datenschutzbeauftragter ist beim Auftragnehmer bestellt:

Datenschutzexperte.de
(PROLIANCE GmbH)
Herr Dominik Fünkner
Leopoldstr. 21
80802 München