AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 DSGVO

zwischen dem Verantwortlichen

Firmenname: .....

Straße/Nr.: .....

PLZ/Ort: .....

– nachfolgend „Auftraggeber“ genannt –

und dem Auftragsverarbeiter

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

– nachfolgend „Auftragnehmer“ genannt –

– nachfolgend zusammen die „Parteien“ genannt –

PRÄAMBEL

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

1.1 Gegenstand dieses Auftragsverarbeitungsvertrages ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG

Die vertraglich vereinbarte Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts anderes ergibt. Vor Verlagerung der Verarbeitung in ein Drittland informiert der Auftragnehmer den Auftraggeber [in schriftlicher Form / in Textform (bspw. per E-Mail)]. Der Auftraggeber kann der Änderung innerhalb von [3 Wochen ab Erhalt] der Information durch den Auftragnehmer in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Die Verlagerung der Verarbeitung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

3. LAUFZEIT

3.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit einer Frist von drei Monaten gekündigt werden. Soweit im Zeitpunkt der Kündigung noch ein Hauptvertrag oder mehrere Hauptverträge, bei denen der Auftragnehmer im Auftrag personenbezogene Daten des Auftraggebers verarbeitet, in Kraft sind, gelten die Bestimmungen dieses Vertrages bis zu der regulären Beendigung des Hauptvertrages/der Hauptverträge fort.

3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. WEISUNG

4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

4.2 Falls Weisungen, die unter Ziffer 1 der Anlage dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung in schriftlicher Form erfolgt.

4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.

4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. 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.

4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer

Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.

5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

6.2 Der Auftraggeber oder von ihm beauftragte Dritte sind – grundsätzlich nach Terminvereinbarung – berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei. 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

6.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

Der Datenschutzbeauftragte des Auftragnehmers ist in der Anlage dieses Vertrages unter Ziffer 3 angeführt, soweit für den Auftragnehmer ein Datenschutzbeauftragter bestellt sein muss oder freiwillig bestellt ist.

8. VERTRAULICHKEIT

8.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

8.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter [durch schriftliche Vereinbarung] für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen.

9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und ein angemessenes Schutzniveau erreicht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen.

9.2 Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird als Anlage in Ziffer 5 diesem Vertrag beigefügt.

9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage unter der Ziffer 5 vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen sind in schriftlicher Form oder einem elektronischen Format zu vereinbaren.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personenbezogener Daten betreffen.

10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.

10.3 Sollten die personenbezogenen Daten, die unter dieser Vereinbarung verarbeitet werden, 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 relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

10.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht feststellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. UNTERAUFTRAGNEHMER

11.1 Vor der Hinzuziehung oder Ersetzung von Unterauftragnehmern informiert der Auftragnehmer den Auftraggeber [in schriftlicher Form / in Textform (bspw. per E-Mail)]. Der Auftraggeber kann der Änderung innerhalb von [3 Wochen] ab Erhalt der Information durch den Auftragnehmer [in schriftlicher Form oder in Textform (bspw. per E-Mail)] begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

11.2 Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.

11.3 Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

11.4 Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der Anlage unter der Ziffer 4 aufgeführten Unterauftragnehmer.

11.5 Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unteraufragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

12.1 Der Auftragnehmer ist nach Abschluss der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat, nach Wahl des Auftraggebers an den Auftraggeber zurückzugeben oder zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung oder Rückgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.

12.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind.

12.3 Der Auftraggeber legt die Maßnahmen zur Rückgabe und / oder Löschung der gespeicherten Daten nach Beendigung des Auftrages individuell durch Weisung fest.

13. HAFTUNG

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen.

14. SCHLUSSBESTIMMUNGEN

14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.

14.2 Die Anlage oder im Falle mehrerer abgeschlossener Hauptverträge die Anlagen zu diesem Vertrag sind wesentlicher Bestandteil desselben.

14.3 Für Änderungen oder Nebenabreden ist die Schriftform oder ein elektronisches Format erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses.

14.4 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.

Für den Auftraggeber

_____, _____

Ort, Datum

_____

[Name/Position des Unterzeichnenden]

Für den Auftragnehmer:

_____, _____

Ort, Datum

_____

[Name/Position des Unterzeichnenden]

ANLAGE ZUM AUFTRAGSVERARBEITUNGSVERTRAG

zwischen

Firmenname: .....

Straße/Nr.: .....

PLZ/Ort: .....

– (nachfolgend „Auftraggeber“ genannt) –

und

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

– (nachfolgend „Auftragnehmer“ genannt) –

– nachfolgend zusammen die „Parteien“ genannt –

1. GEGENSTAND DES AUFTRAGES

1.1. Gegenstand des Auftrages:

☐ 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 FZPModule.

☐ Rahmenvertrag zur Lohnabrechnung und Personalsachbearbeitung im Outsourcing durch die Fa. FZP.

1.2. Umfang, Art und Zweck der Datenverarbeitung (Art. 4 Nr. 2 DSGVO):

☐ 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 Erbringung von Dienstleistungen zur Lohnabrechnung und Personalsachbearbeitung im Outsourcing, laut aktuell vereinbartem Leistungskatalog.

1.3. Art der Daten:

	Datenkategorie	Auflistung konkret verarbeiteter Daten falls abweichend von den Beispielen	Beispiel
☐	Berufliche Kontakt- und (Arbeits-) Organisationsdaten		Name, Vorname, Geschlecht, Anschrift, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Personalnummern, Anwesenheit
☐	Daten zu beruflichen Verhältnissen		Berufsbezeichnung, beruflicher Werdegang, Betriebszugehörigkeit, Aufgaben, Tätigkeiten, Log-File-Auswertung, Eintritts- und Austrittsdaten, Qualifikationen, Beurteilungen, Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe
☐	Private Kontakt- und Identifikationsdaten		Name, Vorname, Geschlecht, Adresse, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer, Datum und Ort der Geburt, Identifikationsnummern, Nationalität
☐	Vertragsdaten		gekaufte Produkte, Datum Kaufvertrag, Kaufpreis, Garantien, Geschäftshistorie von Kunden, Lieferanten und Vertretern
☐	Positionsdaten		GPS, Funknetz-Ortung, Bewegungsprofil, WLAN-Hotspot-Ortung
☐	Daten zu persönlichen Verhältnissen		Daten zum Ehegatten oder Kindern, Familienstand, Portraitfoto, Ehrenamt
☐	Bonitäts- und Bankdaten		Zahlungsverhalten, Bilanzen, Daten von Auskunfteien, Vermögensverhältnisse, Kontoverbindung, Kreditkartennummer
☐	Besonders sensible personenbezogene Daten		rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
☐	Sonstiges		

1.4. **Kreis der Betroffenen:**

	Betroffenengruppe	**Beschreibung**	**Beispiele**
☐	Mitarbeiter des Auftraggebers/des Verantwortlichen	Eigene Mitarbeiter des Auftraggebers/des Verantwortlichen	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
☐	Mitarbeiter anderer Unternehmen	Mitarbeiter anderer Unternehmen, deren personenbezogene Daten für den Auftraggeber/den Verantwortlichen verarbeitet werden	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
☐	Kunden des Auftraggebers/des Verantwortlichen	Jede Person, mit der eine Kunden-Geschäftsbeziehung besteht (mit der jeweiligen verantwortlichen Stelle)	Käufer, Versicherungsnehmer, Mieter, Kunden einer Dienstleistung
☐	Sonstige Geschäftspartner	Jede natürliche Person, mit der eine Geschäftsbeziehung besteht (mit dem Auftraggeber) außer Kunden	Lieferanten, Importeure, Dienstleister, Vermittler, Freelancer
☐	Außenstehende	Jede Person, die in keiner Geschäftsbeziehung mit der jeweiligen Konzerngesellschaft (verantwortlichen Stelle) steht	Besucher, Gäste, Interessenten
☐	Kinder	Personen unter 16 Jahren	

2. WEISUNGSBERECHTIGTE PERSONEN

2.1 Weisungsberechtigte Personen des Auftraggebers sind:

[Name, Organisationseinheit, Funktion, Telefon, E-Mail eintragen]

2.2 Weisungsempfänger beim Auftragnehmer sind:

Bereich Projekte und Support:

Die an den Kunden kommunizierten Projektleiter, Projekt- und Supportmitarbeiter.

Tel.: +49 341 2259922
Fax: +49 341 2259933
E-Mail: info@fzp-beratung.com

Bereich Outsourcing Lohnabrechnung:

Die an den Kunden kommunizierten Lohnabrechner / Sachbearbeiter.

Tel.: +49 341 2259944
Fax: +49 341 2259955
E-Mail: laa@fzp-beratung.com

3. DATENSCHUTZBEAUFTRAGTER

3.1 Datenschutzbeauftragter des Auftraggebers ist:

3.2 Datenschutzbeauftragter des Auftragnehmers ist:

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

4. UNTERAUFTRAGNEHMER UND ERBRACHTE TEILLEISTUNGEN

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Produkte und Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Ob nachstehend genannte Subunternehmen an der Verarbeitung personenbezogener Daten beteiligt sind, entnehmen Sie dem Hauptvertrag und allen nachfolgenden Aufträgen.

4.1 Verarbeiteten Datenkategorien:

- siehe Punkt 1.3

4.2 Beschreibung der Tätigkeit:

- 1st -3rd Level Support für die in den Verträgen mit dem Auftragnehmer eingesetzten Produkten. 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.
- Die Unterauftragnehmer wurden gemäß Art. 28 (4) DSGVO verpflichtet.

Nr.	Unterauftragnehmer (Name, Anschrift)	Beschreibung
1	Sage GmbH Franklinstr. 61-63 60486 Frankfurt / Main	Hersteller Sage Produkte: ERP, HR, uvm.
2	WEKO INFORMATIK GmbH Wilhelm-Nebelung-Strasse 28-29 99734 Nordhausen	Cloud Anbieter
3	SEIBERT MEDIA GmbH Kirchgasse 6 65185 Wiesbaden	Partner für Atlassian-Software; Einsatz von Jira und Confluence zur gemeinsamen Dokumentation im Rahmen des Projektmanagement und gemeinsamer Bearbeitung von Tickets.
4	d.velop digital solution GmbH Kieler Kamp 99 24145 Kiel	Dienstleister für die Einführung von Dokumentenmanagementsystem (D3, dpa)
5	HTK GmbH & Co. KG Nauroth 2 67158 Ellerstadt	OmniSeller - Multi-Channel E-Commerce Lösung mit integriertem PIM-System für Ihren Onlinehandel (Webshop-Schnittstelle zur Sage 100)
6	mobileObjects AG Im Mersch 52 33165 Lichtenau	App für mobile Auftragserfassung mit Schnittstelle zur Sage 100
7	abacus edv-lösungen GmbH & Co.KG Südring 16 19243 Wittenberg	Zusatzmodule zu Sage • Eigenes in Sage integriertes Kassensystem (Weblösung) • Modul für Etikettendruck
8	SPIN GmbH Hellbrunner Str. 11a AT 5020 Salzburg	Kassenlösung
9	LogiSoft GmbH & Co. KG software & consulting Maibachstraße 7 35683 Dillenburg	Zusatzmodul zu Sage: • Rechnungseingangsprüfung • BANF
10	ADVANTAGE SOFTWARE CONSULTING GmbH| Hardenbergstr. 7 10623 Berlin/ Charlottenburg	Zusatzmodul zu Sage: • Rechnungseingangsbuch
11	TS Software GmbH Neugrabenweg | 66123 Saarbrücken	Zusatzmodule zu Sage: • EDI /EDIFACT / EDITEC /EANCOM • NVE / RFID / Palettenetikettierung • Im-und Export für Microsoft Excel für Stammdatenpflege und Auswertungen
12	CHIPSIZE Computer GmbH Podbielskistr. 344| 30519 Hannover	Zusatzmodul zu Sage: • In Sage integriertes Qualitätsmanagement-Modul zur Produktion
13	Global EDI GmbH Koblenzer Str. 83 53177 Bonn	Zusatzmodul zu Sage: • EDI Wandler

14	ecovium GmbH Justus-von-Liebig-Str. 3 31535 Neustadt am Rübenberge	Versandlogistik V-LOG
15	IAS Vollmond GmbH Alfred-Nobel-Allee 41 66793 Saarwellingen	Scannerlösung / Mobile Datenerfassung MDE und BDE für die Sage Produktion
16	SAW Document Solutions GmbH Neefestr. 147 09116 Chemnitz	Dienstleister für DocuWare (Dokumentenmanagementsystem)
17	MS-Consult EDV-Management und Systemberatung GmbH Nibelungenstraße 351 64686 Lautertal	Zusätzliche Sprachmodule
18	CTI Commerzielle und Technische Informationssysteme GmbH Eythstraße 11| 04129 Leipzig	CTI – Soft- und Hardware für Zugangskontrolle und Zeiterfassung, Zeiterfassungsterminals
19	DPS Business Solutions GmbH Am Moosfeld 3 81829 München	Zusatzmodul zu Sage HR: • Bewerbermanagement Smart

5. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Nr.	Prüfpunkt	Antwort
0	**Organisationskontrolle**	
0.1	Wie ist die Umsetzung des Datenschutzes organisiert?	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 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 Datenschutz-bestimmungen ablaufen und wird dies regelmäßig einer Qualitätsprüfung unterzogen?	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?	1x jährlich muss jeder Mitarbeiter eine VOM Datenschutzbeauftragen angebotene Onlineschulung mit anschließender Prüfung absolvieren, Aufstellung von Richtlinien mit datenschutzrechtlichem Bezug
0.5	Wie sind die einschlägigen Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit (z.B. Datenschutz-Folgeabschätzung) dokumentiert?	Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten als Verantwortlicher und Auftragsverarbeiter, Einbeziehung des Datenschutzbeauftragten bei der Dokumentation / Beurteilung von Datenverarbeitungen
0.6	Welche Vorkehrungen zur regel-mäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen werden getroffen?	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?	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?	Abschließbare Büros, Schließregelungen, Regelungen zur Schlüsselvergabe, elektrischer Tierschließer
1.3	Wie werden die Hardwarekomponenten selbst vor Missbrauch geschützt?	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?	regelmäßige Prüfung der Richtlinien / Regelungen wie kontrollierte dokumentierte Schlüsselvergabe.

2.	**Maßnahmen zur Zugangskontrolle**	
2.1	Benutzerverwaltung	
2.1.1	Wie erfolgt die Vergabe von Benutzerzugängen (-accounts)?	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. • Clientzugang • Serverzugang • Zugang zur Anwendung Berechtigung zum Zugriff auf Datenbanken haben nur autorisierte Personen.
2.1.2	Wie wird die Gültigkeit von Benutzerzugängen (-accounts) überprüft?	Unmittelbar mit Änderungen der Aufgabenstellung / Austritt / Versetzung erfolgt eine Anpassung bzw. Löschung der Berechtigungen bzw. Benutzerzugänge, Dokumentation im Rahmen der Netzwerk-dokumentation, regelmäßige Prüfung, zusätzlich vorgegebener Ablauf / Deaktivierungsdatum
2.1.3	Wie werden Benutzerzugänge (-accounts) (inkl. Antrags- und Genehmigungs-verfahren, Änderungsverfahren) dokumentiert?	Schriftliche Dokumentation im Rahmen der Netzwerkdokumentation, schriftliche Dokumentation / Weisungen je nach Berechtigtem
2.1.4	Wie stellen Sie sicher, dass a) die Vergabe von Administrations-zugängen auf die notwendige Anzahl beschränkt ist? b) diese Administratoren die fachlich und persönlich geeignet sind? c) externe Administratoren, Service oder Wartungstechniker persönlich geeignet sind?	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?	Verbindliches Verfahren zur Rücksetzung von Passwörtern durch IT-Administration, Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passwörtern, Vorgabe zur regelmäßigen Änderung 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?	Vorgabe zur regelmäßigen Änderung 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, eine Passwortänderung ist technisch alle 90 Tage vorgegeben, die Vergabe gleicher Passwörter ist technisch ausgeschlossen
2.2.4	Wie erfolgt die Administration von Passwörtern?	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?	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 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 / Standardisierte Vergabeprozesse mit vorgegebenem 4-Augen Zugriffs-berechtigungen anforderungsgerecht und zeitlich Prinzip, Standardisierter Vergabeprozess mit verpflichtender beschränkt vergeben werden?	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?	Dokumentation der Berechtigungen und Rollenvergaben im Rahmen einer Netzwerkdokumentation / individuellen berechtigungsbezogenen Dokumentation
3.3	Wie wird sichergestellt, dass Benutzer ihre Zugriffsberechtigung nicht missbräuchlich verwenden?	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?	Belehrung und Sensibilisierung der Mitarbeiter, Freigabe / Weisung als Voraussetzung, VPN-Verschlüsselung, verschlüsselte Datenübertragung, E-Mail-Verschlüsselung

4.2	Welche Verschlüsselungssysteme werden bei der Weitergabe von personenbezogenen Daten eingesetzt?	Passwortversand über verschlüsselte E-Mails, separate Verschlüsselung von Daten mit höchstmöglicher Verschlüsselung, getrennte Übermittlung von sensiblen Informationen
4.3	Wie wird die Weitergabe personen-bezogener Daten dokumentiert?	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?	Beschränkte Berechtigungen nur für jeweils autorisiertes Personal soweit zwingend erforderlich, individuelle Zugriffsbeschränkung
4.5	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personen-bezogenen Daten aufdecken kann?	Systemseitige Dokumentation / Zugriffsprotokol-lierung, Auswertung von Logfiles
5.	**Maßnahmen zur Eingabekontrolle**	
5.1	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Alle Änderungen an Daten in der Software SAGE werden mittels Protokollierungs-systemen 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 personen-bezogenen Daten durch die damit betrauten Mitarbeiter nur gemäß der Weisung des Auftraggebers erfolgen kann?	Vertragliche Absicherung / datenschutzrechtliche Verpflichtung, Auswahl nach Sorgfaltsgesichts-punkten, Unternehmensrichtlinien, Arbeits- und Organisationsanweisungen und Verpflichtung im Arbeitsvertrag sowie regelmäßige schriftliche Belehrungen und Schulungen.
6.2	Welche Maßnahmen werden getroffen, damit auch ggf. Unterauftragnehmer keine unbefugten Aktivitäten mit den zur Verfügung gestellten Daten durchführt?	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?	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 Datensicherheits-konzept. Komplette Neukonzeption und Daten und Systemen schnellst möglichst zu gewährleisten?	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?	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 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?	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.)
7.5	Welche Maßnahmen werden zur Sicherstellung der Belastbarkeit der Systeme und Dienste und zur Wieder-herstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall getroffen?	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?	Separate Serverlaufwerke für Kundendaten, virtuelle Maschinen, Trennung von Test- und Produktivsystemen, Zugriffsberechtigung, verschlüsselte Speicherung, Verschlüsselung von virtuellen Systemen
9.	**Maßnahmen zur Pseudonymisierung und Anonymisierung**	
9.1	Welche Maßnahmen werden zur Pseudonymisierung und Anonymisierung personenbezogener Daten getroffen?	Kommt für Softwarepflegeleistungen nicht als Option in Betracht. Personenbezogene Daten aus dem Datensafe werden nicht weitergegeben. Fristgerechte Löschung von Daten.

Für den Auftraggeber:
[Name/Position der unterzeichnenden Person einfügen]

_____

Unterschrift/Ort/Datum

Für den Auftragnehmer:
[Name/Position der unterzeichnenden Person einfügen]

_____

Unterschrift/Ort/Datum