Anlage 2

Datenschutzvertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen dem/der

FIRMENNAME

STRASSE HAUSNUMMER

POSTLEITZAHL ORT

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

Brief365 GmbH, Marienstraße 1, 39112 Magdeburg

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

.....

Präambel

(1) Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich auf Grund aller Beauftragungen des Auftraggebers (nachfolgend „**Hauptvertrag**“ genannt) in seinen Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Dritte personenbezogene oder vertrauliche Daten des Auftraggebers verarbeiten.

(2) Sollte nach Beendigung des Hauptvertrages ein Folgevertrag zustande kommen, gelten die Bestimmungen dieser Vereinbarung auch für den Folgevertrag, ohne dass es einer expliziten Verlängerung oder eines Neuabschlusses dieses Vertrages bedarf. Der Folgevertrag ersetzt inhaltlich und begrifflich sodann vollumfänglich den Hauptvertrag im Sinne dieses Vertrages.

Dies vorausgeschickt vereinbaren die Parteien Folgendes:

1 Gegenstand und Dauer der Vereinbarung

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung / Vertrag Brief365-FIRMENNAME-001-A vom DATUM, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage des Hauptvertrages und dieses Datenschutzvertrages.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1.1 Weisung

(1) Eine Weisung erfolgt regelmäßig durch die Leistungsbeschreibung im Hauptvertrag, sie kann vom Auftraggeber jederzeit bei Bedarf in schriftlicher oder elektronischer Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung).

1.2 Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

2.1 Art und Zweck der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO)

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom DATUM.

2.2 Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO)

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

Bitte durch Auftraggeber anpassen!

- Abrechnungsdaten (z.B. Verbrauchs- und Leistungswerte)
- Arbeitszeitdaten (Ist-Arbeitszeit, Soll-Arbeitszeit, Pausen, Urlaub, Sonderurlaub, Fehlzeiten, Krankheitstage, Überstunden)
- Bewerberdaten (Angaben zur Person, Kontaktdaten, Lebenslauf, Foto, Zeugnisse)
- Biometrische Daten (Biometrische Angaben zur betroffenen Person wie z.B. Fingerabdruck, Stimme, Gesichtsmerkmale)
- Bonitätsdaten (Scoringwerte, Zahlungshistorie)
- personenbezogene Fahrzeugdaten (z.B. Halter-, Fahrer-, GPS-Daten)
- Gehaltsdaten (Entgelt, Bonus und Prämien, steuerliche Angaben, Zuschläge)
- Genetischen Daten (Informationen über Genomdaten der betroffenen Person)
- Gesundheitsdaten (z.B. Krankmeldungen, Patientendaten)
- Internetnutzungsdaten (IP-Adresse, Besuchszeit und Datum)
- Kontaktdaten (Name, Telefon, Fax, E-Mail)
- Mitarbeiterdaten (Personalstammdaten, Kontaktdaten, Notfalldaten)

- Protokolldaten (z.B. Logfiles über Nutzungsvorgänge)
- Schadensdaten (Angaben zur Person, Kontaktdaten, Schadensverlauf, Unfallbericht, Zeugen)
- Sozialversicherungsdaten (Krankenkasse, Rentenkasse, Steuerdaten, Kirchensteuermerkmal)
- Teilnehmerdaten (Name, Anschrift, Telefon, E-Mail)
- Verbindungsdaten (Datum und Zeit der Verbindung, Verbindungsteilnehmer)
- Verhaltensdaten (z.B. Verhaltensbeobachtungen, Bewegungsprofil)
- Versicherungsdaten (Angaben zur Person, Kontaktdaten, Vertragsdaten, Gesundheitsangaben, Kontoverbindungen)
- Vertragsdaten (Anschrift, Kontaktdaten, Vertragsinhalte)
- Zahlungsdaten (Kontoinformationen, Kreditkartendaten)

- Berufs-, Branchen-, Geschäfts- und Unternehmensbezeichnung
- Name und Vorname
- Geburtsdatum und –ort
- Titel, akademischer Grad
- Anschrift nach Straße, PLZ, Ort
- Telekommunikationsdaten und weitere Kontaktdaten (z.B. E-Mail, Web-Adresse, Fax)
- Vertragsstammdaten (u.a. Produkt, Kundenhistorie, Abrechnungs- bzw. Zahlungsdaten)
- Daten aus öffentlichen Registern und Verzeichnissen
- freiwillige Angaben der betreffenden Person
- personenbeziehbare Protokolldaten (IP-Adressen, Benutzernahmen usw.)
- Daten, die einem Berufsgeheimnis unterliegen.

2.3 Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO)

Der Auftragnehmer erhält Zugriff auf personenbezogene Daten des Auftraggebers, seiner Mitarbeiter, seiner Kunden, bestehender und potentieller Geschäftspartner sowie Lieferanten verschiedener Branchen (Betroffene) dadurch, dass der Auftraggeber ihm die Daten auf einem SFTP Server oder Web-Portal bereitstellt und ihm einen Zugriff auf die Daten ermöglicht.

3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(4) Der Auftraggeber oder von ihm beauftragte Dritte, sind berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des

Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Weisungsberechtigte Personen des Auftraggebers und Weisungsempfänger beim Auftragnehmer sind schriftlich mit Angabe von Vorname, Name, Organisationseinheit, Telefon im Hauptvertrag bzw. der Leistungsbeschreibung zu benennen.

(2) Für Weisung zu nutzende Kommunikationskanäle: eMail, Post, ergänzend Telefon

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Kopien zur Datensicherung sind von diesem Verbot ausgenommen.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(4) Die Nutzung von mobilen Datenträgern ist zu vermeiden. Personenbezogene Daten sind über sichere verschlüsselte Kanäle auszutauschen.

(5) Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber angemessene Überprüfungen in seinem Bereich durchzuführen.

(6) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutzfolgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

Vorname und Name: _____
E-Mail- Adresse: _____

(7) 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 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(8) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

(9) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(10) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber sowie von ihm beauftragte Dritte - grundsätzlich nach Terminvereinbarung zwei Wochen im voraus - berechtigt sind, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

(11) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(12) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

(13) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

(14) Der Auftragnehmer wird alle mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten über die jeweils aktuellen Weisungen umfassend unterrichten und ihnen untersagen, diese Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten.

(15) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO).

(16) Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb angemessen im Rahmen der Verhältnismäßigkeit.

(17) Als Datenschutzbeauftragte ist beim Auftragnehmer Frau Mandy Herrmann, LGD Datenschutz GmbH, Rogätzer Straße 8, 39106 Magdeburg, Telefon: 0391 5568632-0, datenschutz@lgd-data.de, bestellt.

6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich schwerwiegende Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen oder schwerwiegende Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger schriftlicher Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) erfolgen muss. Der Auftragnehmer trägt dafür Sorge, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt.

(2) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung, Fernwartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern.

(3) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(4) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber und von ihm beauftragte Dritte berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen.

(5) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

(6) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

(7) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) angemessen zu überprüfen.

(8) Zurzeit sind für den Auftragnehmer die in Anlage „Subunternehmer“ mit Namen, teils mit Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
Freiwillig wurden in der genannten Anlage teils auch Subunternehmer, die gemäß Punkt 7. (2) dieses Vertrages nur Nebenleistungen erbringen und deshalb nicht meldepflichtig sind, benannt. Diese Meldung geschieht freiwillig im Hinblick auf den Transparenzgedanken, verpflichtet jedoch nicht zukünftig alle Subunternehmer für Nebenleistungen gemäß Punkt 7. (2) dieses Vertrages zu melden.

(9) Der Auftragnehmer darf Subunternehmer beauftragen. Jede Subbeauftragung ist vorher durch den Auftragnehmer dem Auftraggeber anzuzeigen, wodurch der Auftraggeber die Möglichkeit erhält, dagegen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Hat der Auftraggeber von diesem Einspruchsrecht im Einzelfall Gebrauch gemacht und sollen personenbezogene Daten des Auftraggebers verarbeitet werden, streben Auftragnehmer und Auftraggeber eine einvernehmliche Lösung an, um die Auftragserfüllung sicherzustellen. Hat der Auftraggeber innerhalb einer Frist von 14 Tagen nach Information durch den Auftragnehmer keinen Einspruch eingelegt, so gilt die Genehmigung im Sinne Punkt 7 (1) Satz 1 dieses Vertrages als erteilt.

(10) Stimmt der Auftraggeber einer Subbeauftragung nicht zu und ist der Auftrag dadurch für den Auftragnehmer nicht mehr wirtschaftlich abzubilden, so ist der Auftragnehmer berechtigt den

Auftrag zum Monatsende folgenlos zu kündigen. Hinsichtlich des Nachweises der Unwirtschaftlichkeit trifft den Auftragnehmer keine Beweislast. Es genügt diesbezüglich die Mitteilung der Feststellung, dass die Unwirtschaftlichkeit wegen der Nichtgenehmigung eines Subunternehmers durch den Auftraggeber eingetreten ist.

8 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden mindestens die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste, sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene Risikobewertung durch den Auftraggeber nachweisbar durchgeführt, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

(3) Das zu diesem Vertrag mit zu vereinbarende Datenschutzkonzept des Auftragnehmers stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar. Alternativ kann die beigefügte Anlage „Datenschutzkonzept gemäß Art. 32 GVO“ mit den getroffenen technischen und organisatorischen Maßnahmen angepasst und ergänzt werden, sofern den zuvor ermittelten Risiken damit wirksam begegnet wird.

(4) Das Datenschutzkonzept wird vollumfänglich zum Bestandteil dieses Vertrages.

(5) Der Auftragnehmer hat regelmäßig eine angemessene Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).

(6) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

(7) Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers hinsichtlich des Schutzes der Vertraulichkeit nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

(8) Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO, Datenlöschung

(1) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.
Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Datensicherungen sind davon zunächst ausgenommen und werden im laufenden Betrieb des Auftragnehmers sukzessive gelöscht.

10 Haftung

(1) Es wird grundsätzlich auf Art. 82 DS-GVO verwiesen. Im Übrigen stellt der Auftraggeber den Auftragnehmer von jeder Haftung frei.

11 Sonstiges

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Für Nebenabreden ist grundsätzlich die Schriftform erforderlich.

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(4) Bei etwaigen Widersprüchen gehen die Regelungen dieses Vertrages zur Auftragsverarbeitung abweichenden Regelungen anderer Verträge bezüglich des Datenschutzes vor.

(5) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Vertragsparteien sind im Falle einer unwirksamen Bestimmung dieses Vertrags verpflichtet, über eine Ersatzregelung zu verhandeln, die dem von den Vertragsparteien mit der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt und die rechtlich zulässigen Inhalt hat.

(6) Es gilt deutsches Recht.

Ort,

Auftraggeber	Auftragnehmer
_____	_____
Name:	Name:
Funktion:	Funktion:
_____	_____
Name:	Name:
Funktion:	Funktion:

Anlage Datenschutzkonzept gemäß Art. 32 GVO:

Maßnahme	Umsetzung
M.1 Maßnahmen zur Vertraulichkeit	
M.1.1 Beschreibung der Zutrittskontrolle:	- Zutrittsschutz (personalisierte Keycards und Schlüssel) - Keycard-/ Schlüsselvergabe laut Antrag - Zentrale Verwaltung Zutrittskontrolle (Gebäudemanagement) - Türsicherung (elektrische Türöffner) - Außerhalb der Arbeitszeiten Überwachung des Objektes durch Wachschutz/Pförtner - Aktive Videoüberwachung des Betriebsgeländes - Zugangsregeln für Betriebsfremde (z.B. Besucher, Wartungspersonal)
M.1.2 Beschreibung der Zugangskontrolle:	- Authentifikation über personenbezogene Kennung und Passwort - Automatische Aktivierung von Bildschirmschonern mit Passwort - Einrichtung eines Benutzerstammsatzes pro User - Ablauf Kennwort nach 60 Tagen - Mindestkomplexität und eingeschränkte Wiederverwendbarkeit des Passworts - Verwaltung von Benutzerberechtigungen (z.B. bei Eintritt, Änderung, Austritt) - Einsatz von Firewalls zum Schutz des Netzwerkes - Weitere Festlegungen (Verlassen des Arbeitsplatzes, Umgang mit Passwörtern etc.) sind geregelt in der IT-Richtlinie RL/RI 04-2016
M.1.3 Beschreibung der Zugriffskontrolle:	- projektbezogene differenzierte Vergabe von Berechtigungen - Systemseitige Protokollierung der Vergabe, Änderung oder Löschung von Berechtigungen - Regelmäßige Kontrolle bestehender Berechtigungen - Zeitnahe Aktualisierung bzw. Löschung - Auditing sämtlicher Filesystemzugriffe (betrifft nicht Fremdsysteme) - Erstellen und Einsatz eines Berechtigungskonzepts - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
M.1.4 Beschreibung der Weitergabekontrolle:	- Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet - E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren) - Sichere Transportbehälter und -verpackungen - Falls Datenweitergabe erforderlich ist, erfolgt der Austausch von Daten erfolgt über sicheren Server (sftp) mit

	Verschlüsselung - Verschlüsselung der Daten auf mobilen Datenträgern vor dem Versand - Protokollierung sämtlicher Transferaktionen - Elektronische Signatur
M.1.5 Beschreibung des Trennungsgebots:	- Logische Mandantentrennung (softwareseitig) - Trennung von Produktiv- und Testsystem - Trennung auf Filesystemebene/Zugriff über Rechtesteuerung - Keine Speicherung von Datensätzen außerhalb der Systeme des Mandanten - Eine Zusammenführung von Daten, die für unterschiedliche Zwecke erhoben wurden, erfolgt nicht. - Interne und externe Mandantenfähigkeit
M.1.6 Beschreibung der Pseudonymisierung:	- Trennung von Kundenstammdaten und Auftragsdaten - Trennung von Kontaktdaten und anderen Daten - Die Pseudonymisierung und/oder Anonymiserung von Daten wird fallbezogen und unter Berücksichtigung weiterer Schutzmaßnahmen zur Vertraulichkeit sowie unter Abwägen des Kosten-Nutzen-Aspektes in Abstimmung mit den Verfahrensverantwortlichen und den Auftraggebern vorgenommen. Dies betrifft nicht Systeme des Auftraggebers.
M.1.7 Beschreibung der Verschlüsselung:	- Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard) - Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Einsatz FTAPI - Datentransfertool)
M.2 Maßnahmen zur Integrität	
M.2.1 Beschreibung der Eingabekontrolle:	- Systemseitige Protokollierung der Vergabe, Änderung oder - Löschung von Berechtigungen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.
M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit	
M.3.1 Beschreibung der Verfügbarkeitskontrolle:	- tägliche Datensicherung - schriftliche Regelungen für den DV-Betrieb, die Datensicherung und das Backup - Aktueller Virenschutz (Clients, zentrale Filesysteme, Mail, Internetverkehr) - (USV) Unterbrechungsfreie Stromversorgung und Netzersatzanlage - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort - Firewalls zur Segmentierung von Client- und Servernetzen sowie DMZ-Bereichen

	- Einsatz von Brandfrühsterkennung in den Rechenzentren - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum) - CO2 Feuerlöschgeräte in Serverräumen - Erstellung und Anwendung von IT-Notfallplänen - Klimaanlage in Serverräumen - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen - Schutzsteckdosenleisten in Serverräumen
M.3.2 Beschreibung der raschen Wiederherstellbarkeit:	- IT-Notfallpläne und Wiederanlaufpläne - Regelmäßige und dokumentierte Datenwiederherstellungen
M.4 Weitere Maßnahmen zum Datenschutz	
M.4.1 Beschreibung der Auftragskontrolle:	- Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO. - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
M.4.2 Beschreibung des Managementsystems zum Datenschutz:	- Durchführung regelmäßiger interner Audits - Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen - Managementsystem zum Datenschutz

Anlage Subunternehmer:

Subunternehmer	Anschrift	Auftragsbeschreibung
regiocom SE	Marienstraße 1, 39112 Magdeburg	DevOps
STACKIT - Lidl/Schwarz Gruppe (Schwarz IT KG) ab Mai 2024	Stiftsbergstraße 1, 74172 Neckarsulm	IT-/TK-Dienstleistungen (Cloud, Rechenzentrum)
Paragon Customer Communications Weingarten GmbH	Josef Bayer Straße 5, 88250 Weingarten	Drucken, Kuvertieren, Versandbereitstellung
Pipedrive OÜ	Mustamäe tee 3a, 10615 Tallinn, Estland	CRM-Software
Myra Security GmbH (freiwillige Aufnahme gem. 7 (8) des AVV)	Landsberger Straße 187, 80687 München	Firewall