Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

zwischen

- Verantwortlicher - nachstehend "Auftraggeber" genannt -

und

IIT Gesellschaft für Innovative Informations-Techniken mbH

Im Ermlisgrund 8

76337 Waldbronn

– Auftragsverarbeiter - nachstehend "Auftragnehmer" genannt -

– beide gemeinsam auch "PARTEIEN" genannt -

- jeder einzeln auch "VERTRAGSPARTNER" genannt -

Präambel

Es ist Wille der Parteien, dass alle Voraussetzungen und Anforderungen an eine rechtskonforme Auftragsverarbeitung nach der DSGVO und dem BDSG erfüllt oder geschaffen werden.

Diese Vereinbarung konkretisiert die Verpflichtungen zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Mit dieser Auftragsdatenvereinbarung ersetzen die Parteien alle diesbezüglich vorangegangenen Verträge und Absprachen.

In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

Rangverhältnis

Diese Vereinbarung zur Auftragsverarbeitung ergänzt den Hauptvertrag. Im Falle eines Widerspruchs zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung zur Auftragsverarbeitung vor.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Lizensierung, Installation, Bereitstellung, Schulung, Pflege, Support (auch Remote) im Zusammenhang mit der Software REDIS.win / REDIS.notes / REDAT.kredit / IDEA ***)**

***) Nichtzutreffendes ggf. streichen**

oder

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/ ..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

☒ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist gemäß Hauptbeauftragung gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

oder

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

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum.....

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Lizensierung, Installation, Bereitstellung, Schulung, Pflege, Support (auch Remote) im Zusammenhang mit der Software REDIS.win / REDIS.notes / REDAT.kredit / IDEA ***)**

***) Nichtzutreffendes ggf. streichen**

oder

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

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Art und Kategorien der Daten

Mit Blick auf die Art der für den Auftraggeber verarbeiteten Daten kommen je nach konkreter Verwendung der unter Punkt 2.(1) verwendeten Software des Auftragnehmers nach Wahl des Auftraggebers im Einzelfall (Weisung) grundsätzlich sämtliche denkbaren Arten und Kategorien personenbezogener Daten in Betracht; insbesondere (aber nicht ausschließlich) beispielsweise auch „besondere Kategorien“ personenbezogener Daten gem. Art. 9 DS-GVO, personenbezogene Daten gem. Art. 10 DS-GVO und/oder womöglich auch Daten, die einer besonderen berufsrechtlichen Verschwiegenheitsverpflichtung im Sinne von § 203 StGB aus weiteren Rechtsnormen unterliegen.

Ebenso unterliegen auch die Kategorien betroffener Personen der uneingeschränkten und alleinigen Disposition des Auftraggebers, sodass insbesondere (aber nicht ausschließlich) Beschäftigte, Interessenten, Lieferanten, Kunden, Patienten, Mandanten, Besucher und/oder Antragsteller als betroffene Personen nach Wahl des Auftraggebers in Betracht kommen können.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung, sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [***siehe Anlage 1***].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) ☒ Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Jürgen Recha, c/o interev GmbH, Robert-Koch-Straße 55, 30853 Langenhagen, Telefon +49 511 89 79 84 10, E-Mail: datenschutz@interev.de bestellt.

b) ☒ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

c) ☒ Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftrag gebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) ☒ Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen ist gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [***siehe Anlage 1***] sicherzustellen.

e) ☒ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) ☒ Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) ☒ Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse, sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) ☒ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

i) ☒ Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer ein Verzeichnisses der Verarbeitungstätigkeiten zu führen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO [***siehe Anlage 2***].

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Bei Vorliegen eines unangemessen hohen Aufwand (Häufigkeit oder Ausmaß) bei der Umsetzung der Kontrollrechte, kann der Auftraggeber einen angemessenen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken

berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftraggeber benennt die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen [**siehe Anlage 3**].

10. Fernwartung [sofern zutreffend, ansonsten streichen]

(1) Der Auftragnehmer wird bei der Durchführung von Fernwartungsmaßnahmen ausschließlich auf Daten zugreifen, die Gegenstand der vereinbarten Fernwartung und für deren Durchführung zwingend erforderlich sind. Er wird keine Kopien anfertigen. Der Auftragnehmer darf ferner keine eigenen Test- und Wartungsprogramme dauerhaft auf dem fernzuwartenden System ablegen. Eine Speicherung von Daten auf Rechnern außerhalb des Bereiches des Auftraggebers erfolgt nur auf dessen Weisung.

(2) Der Auftragnehmer wird den mit der Fernwartung betrauten Personen nur die zur Durchführung der konkreten Aufgaben nötigen Berechtigungen erteilen. Der Auftraggeber definiert hierfür Vorgaben, die der Auftragnehmer einzuhalten hat oder er richtet entsprechende Benutzerkonten ein.

(3) Das per Fernwartung zu wartende System wird jeweils für jeden Wartungsfall durch einen Mitarbeiter des Auftraggebers freigegeben. Dafür wird ein Mitarbeiter des Auftraggebers dem Auftragnehmer je Sitzung ein neu vergebenes Zugangskennwort entweder telefonisch oder mittels E-Mail zuverlässig verschlüsselt übermitteln.

(4) Sofern technisch möglich, erfolgt die Fernwartung innerhalb von Testumgebungen. Eine Fernwartung auf Produktivsystemen erfolgt ausschließlich dann, wenn ein Wartungsziel anderweitig nicht erreicht werden kann.

(5) Wird die Verbindung mehr als zwanzig Minuten vom Auftragnehmer nicht genutzt, wird sie durch den Auftraggeber unterbrochen und bei Bedarf nach dem oben beschriebenen Verfahren erneut hergestellt.

(6) Vor einem Zugriff auf personenbezogene Daten im Rahmen der Fernwartung holt der Auftragnehmer in jedem Einzelfall die Zustimmung eines Systemverantwortlichen des Auftraggebers ein. Die elektronische Übertragung oder physische Übertragung personenbezogener Daten auf einen Datenträger an den Auftragnehmer erfolgt nur auf Weisung des Auftraggebers.

(7) Bei der Wartung oder Fernwartung übertragenen oder auf Datenträger gespeicherte Daten dürfen nicht an Dritte weitergegeben werden und müssen vollständig gelöscht werden, sobald sie nicht mehr zur Erfüllung der vertraglich vereinbarten Wartungsarbeiten benötigt werden.

(8) Der Auftragnehmer gewährleistet, die Fernwartung ausschließlich von Standorten innerhalb der Mitgliedsstaaten der Europäischen Union oder des Europäischen Wirtschaftsraumes aus durchzuführen.

(9) Der Auftraggeber und der Auftragnehmer dürfen eine Fernwartungsmaßnahme bei Unklarheiten über deren rechtmäßigen Verlauf unverzüglich abbrechen.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort, Datum	Ort, Datum
Name in Druckbuchstaben, Position	Ralph Grobert, Geschäftsführer Name in Druckbuchstaben, Position
Unterschrift und Stempel Auftraggeber	Unterschrift und Stempel Auftragnehmer

IIT Gesellschaft für Innovative Informations-Technik mbH
Ermlisgrund 8 · D-76337 Waldbronn

Anlage 1 – Technisch-organisatorische Maßnahmen der IIT Gesellschaft für Innovative Informations-Techniken mbH

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

a) Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen, um einen unbefugten Zutritt zu den Räumlichkeiten, in denen die Daten verarbeitet werden, zu verhindern:

- Elektronische und mechanische Zutrittskontrolle.
- Besucher werden von der besuchten Person direkt vom Eingangsbereich abgeholt und durch das Haus an die entsprechende Stelle geführt und nach Besuchsende bis zum Ausgang begleitet.
- Schlüsselregelung (Schlüsselausgabe etc.).
- Sicherheitsbeschläge.

b) Zugangskontrolle

Technische bzw. organisatorische Maßnahmen, um die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern:

- Der Zugang zu den Datenverarbeitungssystemen kann nur mittels einer in der Domäne vergebenen Benutzerkennung und persönlichem Passwort erfolgen.
- Regelmäßig „erzwungener Passwortwechsel“: Kennwortänderung mit entsprechenden Anforderungen (8 Stellen, Sperrung der letzten 7 Passwörter). Eine Weitergabe von persönlichen Kennwörtern ist strengstens untersagt.
- Nach 5 fehlerhaften Passworteingaben erfolgt automatisch eine Sperrung der Benutzerkennung. Die Sperre kann nur durch einen Systemadministrator aufgehoben werden.
- Sämtliche Sperrungen von Benutzerkennungen werden protokolliert.
- Einsatz Anti-Viren-Software.
- Einsatz einer Hardware-und Software-Firewall.
- Fernwartung via VPN-Tunnel und/oder Token.

c) Zugriffskontrolle

Technische bzw. organisatorische Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Zugriffsberechtigung wird durch Einrichtung einer persönlichen Mitarbeiterkennung hergestellt, welche durch den Systemadministrator vergeben wird.
- Der Systemadministrator kann auf Weisung die Zugriffsmöglichkeit durch Passwortlöschungen oder -änderungen und Prioritätenvergabe kontrollieren.
- Anzahl der Administratoren ist auf das „Notwendigste“ reduziert.
- Zugriff auf die Serversysteme haben ausschließlich Mitarbeiter mit entsprechenden Administrator-Rechten.

- Physische Löschung von Datenträgern vor Wiederverwendung.
- Einsatz von Aktenvernichtern bzw. zertifizierten Dienstleistern.
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel.

d) Trennungskontrolle

Technische bzw. organisatorische Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung von Test- und Produktivsystemen.
- Trennung nach Mandanten.
- Festlegung von Datenbankrechten.

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

a) Weitergabekontrolle

Technische bzw. organisatorische Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist bzw. stattgefunden hat:

- Bereitstellung von gesicherten Verbindungen wie https, sftp.
- Datenträger und Daten in Papierform mit personenbezogenen Daten werden, sofern sie nicht gerade in Bearbeitung sind, gesichert aufbewahrt.
- Die nicht mehr benötigten Datenträger (einschließlich in Papierform) werden qualifiziert entsorgt.
- Beim physischen Transport: sorgfältige Auswahl des Personals.
- Einrichtung von VPN-Tunneln.
- Sicherungsdateien werden vom System regelmäßig erstellt.
- Sicherungen werden mit Zeitpunkt und Datum fixiert und zudem auch räumlich getrennt aufbewahrt.

b) Eingabekontrolle

Technische bzw. organisatorische Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, dort verändert oder aus diesen entfernt worden sind:

- Eingegebene, personenbezogene Daten können nachträglich zurückverfolgt und festgehalten werden.
- Alle Mitarbeiter sind durch ihre Mitarbeiterkennungen im Datensatz identifizierbar.
- Das Löschen gespeicherter Daten ist nur durch einen befugten Personenkreis möglich.

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

a) Verfügbarkeitskontrolle

Der Auftragnehmer ergreift unter anderem die folgenden technischen bzw. organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Das Gebäude ist gegen aus einem Blitzschlag resultieren Schäden abgesichert.
- Die Serversysteme und produktiven Arbeitsplätze sind gegen Stromausfall abgesichert.
- Von den Produktivsystemen werden regelmäßig im Rahmen der Datensicherung Sicherungskopien der Datenbestände erstellt.
- Im laufenden Betrieb erfolgt die Speicherung der Daten auf Raid-Systemen oder gespiegelten Datenbanksystemen.
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort.
- Klimaanlage in Serverräumen.
- Schutzsteckdosenleisten in Serverräumen.
- Feuerlöscher vorhanden.
- Testen von Datenwiederherstellung.

b) Rasche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass nach einer Unterbrechung schnellstmöglich der Datenzugriff wiederhergestellt wird:

- Vorhandenes Backup & Recoverykonzept.

4. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

a) Datenschutz-Management

Maßnahmen, die gewährleisten, dass die Anforderung der DSGVO nachprüfbar umgesetzt wurde:

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung.
- Regelmäßige Sensibilisierung der Mitarbeiter durch den externen Datenschutzbeauftragten im Rahmen des „DATENSCHUTZ-PARCOURS“.
- Als externer Datenschutzbeauftrager wurde bestellt: Herr Jürgen Recha, c/o interev GmbH, Robert-Koch-Straße 55, 30853 Langenhagen, Telefon +49 511 89 79 84 10, e-mail: datenschutz@interev.de.

b) Incident-Response-Management

Maßnahmen, die gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern dessen Daten betroffen waren:

- Einsatz von Firewall und regelmäßige Aktualisierung.
- Einsatz von Spamfilter und regelmäßige Aktualisierung.
- Einsatz von Virenscanner und regelmäßige Aktualisierung.

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

Maßnahmen, die gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden (privacy by design / privacy by default):

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen.
- Manuelle Softwareunterstützung.
- Manuelle Löschung nach gesetzlicher Vorgabe.
- Manuelle Löschung auf Anforderung.

d) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Abschluss der notwendigen Vereinbarung zur Auftragsvereinbarung.
- Verpflichtung der Mitarbeiter auf Datengeheimnis.
- Auswahl eines Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- Vereinbarung wirksamer Kontrollrechte.

Anlage 2 – Liste der Unterauftragnehmer des Auftragnehmers

Name/Firma Unterauftragnehmer	Anschrift/Land	Leistung

Anlage 3 – Weisungsberechtigte Personen

Person 1 beim Auftraggeber

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
EMAIL Adresse	

Person 2 beim Auftraggeber (optional)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
EMAIL Adresse	