Allgemeine Nutzungsbedingungen für die Nutzung des EQUITEDO-Systems

FIBS - Forschungsinstitut für Inklusion durch Bewegung und Sport gGmbH, Paul-R.-Kraemer-Allee 100, 50226 Frechen (nachfolgend als „**EQUITEDO**“ bezeichnet) bietet Reittherapeutinnen und Reittherapeuten die Nutzung des EQUITEDO-Systems zu den nachfolgenden Nutzungsbedingungen an.

Mit der Registrierung bei EQUITEDO geben Sie als Vertragspartner oder Vertragspartnerin (nachfolgend als „der VP“ bezeichnet) ein Angebot zum Abschluss des nachfolgenden Servicevertrages ab. Der Vertrag kommt durch Übersendung der Auftragsbestätigung durch EQUITEDO zustande. Daneben kommt ein Vertrag auch dann zustande, wenn EQUITEDO nach Zugang des Angebotes des VP mit der Ausführung der Leistungen beginnt.

Abweichende Allgemeine Geschäftsbedingungen des VP werden auch dann nicht Vertragsinhalt, wenn EQUITEDO ihrer Einbeziehung nicht ausdrücklich widerspricht.

A. Servicevertrag

1. Präambel

EQUITEDO bietet ein cloudbasiertes Softwaresystem für Reittherapeutinnen und Reittherapeuten an, welches insbesondere ein Dokumentations- und Evaluationstool zur Messung von Effekten pferdgestützter Therapien umfasst und die Arbeit von Reittherapeutinnen und Reittherapeuten unterstützen soll. Das System ermöglicht es, Therapieverläufe klientenbezogen zu dokumentieren und zu evaluieren. Es bietet neben einer Klient*innenverwaltung über Hilfsmittel zur Terminorganisation bis hin zu Abrechnungsfunktionen verschiedene Funktionen für die tägliche Arbeit. Eine Übersicht der Funktionen ist auf der Internetseite von EQUITEDO (www.equitedo.com) abrufbar. Die Nutzung des Systems (nachfolgend „**Service**“ genannt) erfolgt als webbasierte Software-as-a-Service-Lösung bzw. mittels einer Progressive Web Applikation (PWA). Der VP möchte den Service für berufliche Zwecke im Rahmen ihrer gewerblichen oder selbständigen Tätigkeit nutzen. Vor diesem Hintergrund schließen die Parteien diesen Vertrag.

2. Vertragsgegenstand

2.1. Gegenstand dieses Vertrages ist die Nutzung des Service durch den VP während der Dauer dieses Vertrages. Das vom VP gebuchte Leistungspaket (Single-, 5er oder Multi-Account) ergibt sich aus der Auftragsbestätigung.

3. Leistungsumfang

3.1. Auf Grundlage dieses Vertrages ist der VP dazu berechtigt, den Service im beauftragten Umfang während der Dauer dieses Vertrages zu nutzen.

3.2. Der VP darf den von EQUITEDO bereitgestellten Service nur zu internen, eigenen geschäftlichen Zwecken über den für den VP von EQUITEDO eingerichteten Benutzerzugang nutzen.

3.3. EQUITEDO stellt dem VP während der Laufzeit dieses Vertrages die Nutzung einer PWA über die Web-Benutzerschnittstelle (User Interface) in der jeweils aktuell von EQUITEDO freigegebenen Softwareversion bzw. über die PWA für mobile Endgeräte am Routerausgang des Rechenzentrums, in dem die Software für den vertragsgegenständlichen Ser-

vice gehostet wird, während der vereinbarten Betriebszeit zur Verfügung. Die für die Nutzung de PWA auf den Servern erforderliche Rechenleistung und der für die Datenverarbeitung erforderliche Speicherplatz werden von EQUITEDO bereitgestellt.

4. Mitwirkungspflichten deSVP

4.1. Der VP wird EQUITEDO bei der Erbringung der vertraglichen Leistungen in angemessenem Umfang unterstützen. Insbesondere wird der VP sämtliche zur ordnungsgemäßen Leistungserbringung erforderlichen Mitwirkungshandlungen rechtzeitig, vollständig und fachlich ordnungsgemäß erbringen.

4.2. Der VPdie internen IT-Systeme nach den allgemein anerkannten Regeln der Technik eigenverantwortlich einzurichten, gegen Schadsoftware bzw. unbefugte Eingriffe Dritter abzusichern, instand zu halten, zu patchen und bei Bedarf zu erneuern. Insbesondere hat der VP sicherzustellen, dass seine IT-Systeme den jeweiligen Systemvoraussetzungen von EQUITEDO zur Nutzung des Service entsprechen. Dies gilt im Falle der Nutzung der PWA u. a. für den verwendeten Internetbrowser (Microsoft Edge, Safari, Mozilla Firefox oder Google Chrome) in der jeweils aktuellen und max. letzten Vorgängerversion.

4.3. Der VP wird Störungen unverzüglich gemäß Ziff. 6.2 melden. Er wird EQUITEDO bei der Fehlersuche aktiv unterstützen.

4.4. Der VP hat jede missbräuchliche Nutzung des Service sowie der dem Service zugrundeliegenden Hard- und Software auf Seiten EQUITEDO zu unterlassen. Eine Nutzung des Service zu rechtswidrigen Zwecken und/oder die Übermittlung rechtswidriger Inhalte über den Service sind untersagt.

4.5. Die Erfüllung von Mitwirkungspflichten des VP ist vertragliche Leistungspflicht und grundlegende Voraussetzung für die Leistungserbringung durch EQUITEDO. EQUITEDO ist berechtigt, den durch vom VP verursachte Leistungsbehinderungen entstehenden Mehraufwand, insbesondere für eine verlängerte Bereitstellung von Personal oder zusätzliche Sachmittel, zu den üblichen Sätzen von EQUITEDO gesondert in Rechnung zu stellen. Etwaige Leistungsfristen von EQUITEDO verlängern sich der Dauer der Leistungsbehinderung entsprechend, ggf. zuzüglich erforderlicher und angemessener Wiederanlauffristen.

5. Verfügbarkeit

5.1. EQUITEDO stellt den Service während der Laufzeit dieses Vertrages in der vorgesehenen Betriebszeit zur Nutzung durch den VP zur Verfügung („Betriebszeit“).

5.2. Die Verfügbarkeit des Service beträgt 99,5 % im Monatsmittel.

6. Service und Support

6.1. EQUITEDO wird die dem Service zugrundeliegende Software während der Laufzeit dieses Vertrages pflegen und jeweils den aktuell freigegebenen Programmstand bzw. der jeweils aktuelle Service zur Nutzung durch den VP bereitstellen. Die Pflege umfasst die Erhaltung und Wiederherstellung der Betriebsbereitschaft, die Diagnose und Beseitigung von Mängeln sowie ggf. funktionserweiternde Maßnahmen.

6.2. Der VP ist verpflichtet, Funktionsausfälle und sonstige Störungen des Service EQUITEDO unverzüglich und so präzise wie möglich anzuzeigen. Die Störungsmeldung durch den erfolgt über ein von EQUITEDO eingerichtete Störungsmeldungssystem; dieses ist erreichbar unter **equitedo@fi-bs.de** In der Störungsmeldung ist die Störung detailliert zu beschreiben:

- Beschreibung der Störung (nach Möglichkeit Screenshots beizufügen)
- Wann ist die Störung aufgetreten?
- Wie wirkt sich die Störung aus?

6.3. EQUITEDO wird Störungen in Abhängigkeit von der jeweiligen Klassifizierung der Störung bzw. des Fehlers bearbeiten.

6.4. Soweit nicht explizit abweichend vereinbart, schuldet EQUITEDO unter diesem Vertrag keine weitergehenden Schulungs-, Beratungs-, Unterstützungs-, Entwicklungs- und Einrichtungsleistungen.

7. Haftung

7.1. Für vorsätzlich und grob fahrlässig verursachte Schäden haftet EQUITEDO unbeschränkt.

7.2. EQUITEDO haftet nicht für leicht fahrlässige Pflichtverletzungen, sofern nicht Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Garantien betroffen oder Ansprüche nach dem Produkthaftungsgesetz berührt sind. Unberührt bleibt ferner die Haftung für die Verletzung von Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der VP regelmäßig vertrauen darf („vertragswesentliche Pflichten“). Gleiches gilt für Pflichtverletzungen der Erfüllungsgehilfen von EQUITEDO.

7.3. Soweit nach vorstehender Ziff. 7.2 eine Haftung für die leicht fahrlässige Verletzung vertrags-wesentlicher Pflichten besteht, ist diese auf den bei Geschäften gleicher Art typischen und vorhersehbaren Schaden begrenzt, sofern der Schaden nicht in der Verletzung einer Garantie oder des Lebens, des Körpers oder der Gesundheit besteht bzw. Ansprüche nach dem Produkthaftungsgesetz betrifft.

8. Vergütung

8.1. Die vom VP zu zahlende Vergütung richtet sich nach den bei Vertragsschluss vereinbarten und in der Auftragsbestätigung bestätigten Konditionen.

8.2. Laufende Vergütungen werden monatlich zum 1. Werktag des Leistungsmonats mittels Lastschrifteinzug oder Kreditkartenzahlung fällig.

8.3. Alle genannten Preise verstehen sich zzgl. der jeweils geltenden gesetzlichen Umsatzsteuer.

9. Testzeitraum, Vertragslaufzeit, Kündigung

9.1. Die Vertragslaufzeit beginnt mit dem Zustandekommen dieses Vertrages und wird auf unbestimmte Zeit geschlossen.

9.2. EQUITEDO bietet dem VP unentgeltlich einen sechswöchigen Testzeitraum an. Innerhalb des Testzeitraums kann der VP den Vertrag jederzeit durch Erklärung in Textform mit sofortiger Wirkung kündigen. Setzt der VP die Nutzung des Systems über den Testzeitraum hinaus fort, ist der Vertrag ordentlich kündbar mit einer Frist von vier Wochen zum Ende des Kalendermonats.

9.3. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

9.4. Kündigungen unter diesem Vertrag bedürfen der Textform.

10. Vertraulichkeit

10.1. Die Parteien verpflichten sich, sämtliche im Rahmen der Durchführung dieses Vertrages erlangten betriebsinternen technischen und kaufmännischen (z. B. Preise, Kosten u. ä.) Informationen einschließlich solcher Informationen, die (a) im Rahmen der Nutzung des Service ausgetauscht oder zugänglich werden, (b) im Rahmen von Zugriffsmöglichkeiten auf Datenbanken erhalten werden oder (c) sich aus etwaigen Mustern ergeben - nachfolgend zusammen als „Informationen" bezeichnet - nur für die Zwecke und im Rahmen der Bestimmungen dieses Vertrags zu nutzen, sie im Übrigen jedoch

- vertraulich zu behandeln und Dritten ohne vorherige schriftliche Genehmigung durch die jeweils andere Partei nicht zugänglich zu machen und

- nur solchen Personen zugänglich zu machen, die sie für die Zwecke dieses Vertrags benötigen und die zur Geheimhaltung verpflichtet worden sind.

10.2. Die vorstehenden Verpflichtungen entfallen für solche Informationen, für welche die empfangende Partei nachweist, dass sie

- vor dem Empfang hiervon Kenntnis hatte; oder

- der Öffentlichkeit vor dem Empfang zugänglich waren, oder

- der Öffentlichkeit nach dem Empfang zugänglich wurden, ohne dass sie hierfür verantwortlich war, oder

- ihr zu einem beliebigen Zeitpunkt von einem Dritten ohne Verpflichtung zur Geheimhaltung zugänglich gemacht worden sind, oder

- von der empfangenen Partei bereits unabhängig entwickelt worden sind, wobei die unabhängige Entwicklung schriftlich nachzuweisen ist.

10.3. Die Verpflichtungen gemäß dieser Ziff. 10 gelten nach Beendigung dieses Vertrages fort.

11. Datenschutz

11.1. Der VP wird im Rahmen des Vertrages und der Nutzung des Service die dem VP obliegenden datenschutzrechtlichen Verpflichtungen, insbesondere gemäß DS-GVO und BDSG strikt beachten.

11.2. Die Verarbeitung von Klientendaten im Rahmen des Service durch EQUITEDO erfolgt ausschließlich im Auftrag und nach Weisung des VP auf Grundlage der Auftragsverarbeitungsvereinbarung nach **ANLAGE 1 – AUFTRAGSVERARBEITUNG**.

12. Höhere Gewalt

12.1. EQUITEDO ist von der Verpflichtung zur Leistung aus diesem Vertrag befreit, wenn und soweit die Nichterfüllung von Leistungen auf das Eintreten von Umständen höherer Gewalt nach Vertragsabschluss zurückzuführen ist.

12.2. Als Umstände höherer Gewalt gelten z. B. Kriege, Streiks, Unruhen, Enteignung, Sturm, Überschwemmung und sonstige Naturkatastrophen sowie sonstige von EQUITEDO nicht zu vertretende Umstände (insbesondere Wassereinbrüche, Stromausfälle und Unterbrechung oder Zerstörung datenführender Leitungen).

12.3. Jede Vertragspartei hat die andere Vertragspartei über den Eintritt eines Falles von höherer Gewalt unverzüglich und in schriftlicher Form in Kenntnis zu setzen und die andere

Vertragspartei in gleicher Weise zu informieren, sobald das Ereignis höherer Gewalt nicht mehr besteht.

13. Nachunternehmer

EQUITEDO ist dazu berechtigt, die unter diesem Vertrag geschuldeten Leistungen durch Nachunternehmer erbringen zu lassen. Dies gilt insbesondere für den technischen Betrieb von zur Realisierung des Service genutzten Rechenzentren.

14. Schlussbestimmungen

14.1. Allgemeine Geschäftsbedingungen des VP finden keine Anwendung.

14.2. Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts (CISG) und des Deutschen Internationalen Privatrechts.

14.3. Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen dieses Vertrags bedürfen zu ihrer Wirksamkeit der Textform und müssen von Vertretern beider Parteien bestätigt werden.

14.4. Der VP kann Zurückbehaltungs- und Leistungsverweigerungsrechte nur bei unbestrittenen oder rechtskräftig festgestellten Gegenansprüchen geltend machen. Eine Aufrechnung ist ebenfalls nur mit unbestrittenen oder rechtskräftig festgestellten Gegenansprüchen zulässig.

14.5. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Anstelle der unwirksamen Bestimmung verpflichten sich die Parteien, die Regelung zu vereinbaren, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

14.6. Gerichtsstand ist Köln.

15. Anlagen

ANLAGE 1 – AUFTRAGSVERARBEITUNG

gez. FIBS - Forschungsinstitut für Inklusion durch Bewegung und Sport gGmbH

gez. Vertragspartner / Vertragspartnerin

B. ANLAGE 1 – AUFTRAGSVERARBEITUNG

Auftragsverarbeitungsvertrag

zwischen EQUITEDO (nachfolgend als „**Auftragnehmer**“ bezeichnet) und Vertragspartner oder Vertragspartnerin (nachfolgend als „**Auftraggeber**“ bezeichnet).

Der Auftragnehmer stellt dem Auftraggeber auf Grundlage des Cloud Servicevertrages (im Folgenden: "**Hauptvertrag"**) das EQUITEDO-System zur Nutzung bereit, mittels dessen der Auftraggeber die Durchführung reittherapeutischer Therapiemaßnahmen dokumentieren und abrechnen kann. Teil der Durchführung des Hauptvertrags ist die Verarbeitung personenbezogener Daten im Sinne der Datenschutzgrundverordnung ("**DS-GVO**"). Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag:

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags zum Datenumgang ist die technische Bereitstellung der im Hauptvertrag definierten Serviceleistungen einschließlich des Hosting der vom Auftraggeber auf den Systemen des Auftragnehmers verarbeiteten Daten.

(2) Die Dauer dieses Auftrags entspricht der Laufzeit des Hauptvertrages.

§ 2 Konkretisierung des Auftragsinhalts

(1) Der Auftrag des Auftragnehmers betrifft die technische Bereitstellung und Pflege des EQUITEDO-Systems, in dem der Auftragnehmer personenbezogene Daten verarbeitet.

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 Artt. 44 ff. DS-GVO erfüllt sind.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenkategorien:

- Personenstammdaten
- Kommunikationsdaten
- Vertragsstammdaten
- Therapieverlaufsdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Terminplanungsdaten

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Klientinnen und Klienten des Auftraggebers.

§ 3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen.

Die bei Vertragsschluss vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in **Anhang 1** dokumentiert.

(2) 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.

§ 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 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Bestellung eines Datenschutzbeauftragten:

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Dieser ist erreichbar unter: Datenschutz@gold-kraemer-stiftung.de oder unter der Postadresse des Auftragnehmers mit dem Zusatz „der Datenschutzbeauftragte“.

b) Vertraulichkeit

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 Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) 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.

e) 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 Auftrags-

verarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) 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.

§ 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 und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen 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) Im Zeitpunkt des Vertragsschlusses hat der Auftragnehmer folgende Unterauftragnehmer beauftragt, deren Einbeziehung der Auftraggeber zustimmt:

Firma	**Sitz**	**Leistung**
Host Europe GmbH	Köln	Rechenzentrumsdienstleistungen
Sawatzki Mühlenbruch GmbH	Essen	Softwareentwicklung / Pflege

(3) Der Auftragnehmer darf Unterauftragnehmer nur nach vorheriger dokumentierter Zustimmung des Auftragnehmers beauftragen. Die Zustimmung wird hiermit erteilt, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt,
- 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 DS-GVO zugrunde gelegt wird.

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der Zustimmung des Hauptauftragnehmers.

§ 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 DS-GVO 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) Der Nachweis solcher Maßnahmen kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 8 Mitteilung von Verstößen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- 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
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

§ 9 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens 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.

§ 10 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) Mit Beendigung der Leistungsvereinbarung hat der Auftraggeber die Daten zu exportieren. Der Auftragnehmer ist verpflichtet, ihm die Daten insoweit bereitzustellen und nach erfolgtem Download des Auftraggebers nach Vertragsbeendigung 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.

Anhang 1 – Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:
  - Rechenzentrum verfügt über elektronische Zutrittskontrollsysteme und Personal zur Überwachung des Zutritts nur für autorisierte Personen
  - Rechenzentrum verfügt über Videoüberwachung und Einbruchsmeldeanlage
  - Rechenzentrum verfügt über automatische Alarmierung
  - Restriktive Zutrittsregelung
- Zugangskontrolle
  Keine unbefugte Systembenutzung:
  - Auftragnehmer verfügt über Passwortrichtlinie
  - automatische Sperrmechanismen,
  - Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:
  - Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte,
  - Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:
  - Mandantenfähigkeit des Systems;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  - Hierüber entscheidet der Auftraggeber bei der Nutzung des Systems.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:
  - Nutzung von Verschlüsselungstechnologien;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
  - Protokollierung;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:
  - Backup-Strategie,
  - unterbrechungsfreie Stromversorgung (USV) des Rechenzentrums
  - Einsatz von Sicherheitssoftware (Virenschutz)
  - Firewall
  - Notfallplan;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.