LiMS - Vertrag über die Auftragsverarbeitung

Zwischen

Name + Adresse MO

(nachfolgend „**Auftraggeber**“)

und

Name + Adresse MO / DOSB

(nachfolgend „**Anbieter**“)

§ 1 Auftrag und Festlegungen zur Verarbeitung

1.1. Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „**AVV**“) konkretisiert für alle Verarbeitungen die datenschutzrechtlichen Rechte und Pflichten der Parteien, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend „**Hauptvertrag**“) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch den Anbieter für den Auftraggeber kommt.

1.2. Dieser AVV kommt mit all seinen Bestandteilen zur Anwendung, wenn der Auftraggeber den Anbieter zur Verarbeitung personenbezogener Daten (nachfolgend „**Daten**“) im Auftrag gemäß Art. 28 DSGVO verpflichtet hat. Dabei bildet dieser AVV den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

1.3. Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.

1.4. Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (nachfolgend „**Festlegungen**“) werden vor Beginn der Verarbeitung in Anlagen zum AVV (nachfolgend „**Anlagen**“) geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorien von Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (nachfolgend „**TOM**“).

1.5. Die Anlagen sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Anlagen der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den Anlagen auf den AVV Bezug genommen, so ist der AVV mit all seinen Bestandteilen gemeint.

§ 2 Verantwortlichkeit und Verarbeitung auf Weisung

2.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Anbieter sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ gemäß Art. 4 Nr. 7 DSGVO).

2.2. Der Anbieter handelt wegen der Verarbeitung der Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Wird der Auftraggeber als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Auftraggebers aus dieser Auftragsverarbeitung für den Dritten unmittelbar als Weisungen des Auftraggebers im Verhältnis zum Anbieter, sofern diese Verpflichtungen strenger sein sollten als diejenigen aus diesem AVV. Der Auftraggeber wird den Anbieter über solche Anforderungen Dritter an die Auftragsverarbeitung schriftlich in Kenntnis setzen.

2.3. Der Anbieter berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (nachfolgend „Sperrung“), wenn der Auftraggeber dies anweist und dies sonst vom Weisungsrahmen umfasst ist.

2.4. Der Anbieter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz oder diesen AVV verstößt. Der Anbieter darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Anbieter ablehnen.

2.5. Die Parteien benennen gegenseitig in Textform einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren. Der Datenschutzbeauftragte des Anbieters findet sich unter www.dosb.de/ueber-uns/datenschutz.

2.6. Der Anbieter gewährleistet, dass die zur Verarbeitung der Daten befugten Personen (a) die Weisungen des Auftraggebers kennen und diese beachten, sowie (b) sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

2.7. Wird der Auftraggeber als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Anbieters aus diesem AVV auch unmittelbar im Verhältnis zwischen dem Dritten und dem Anbieter. Dies gilt für alle Leistungen des Anbieters, welche dieser im Auftrag des Auftraggebers gegenüber dem Dritten erbringt. Insbesondere stehen dem Dritten die Kontroll- und Informationsrechte aus § 8 unmittelbar gegenüber dem Anbieter zu.

§ 3 Sicherheit der Verarbeitung

3.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten in einer Anlage zu diesem AVV (nachfolgend „**Anlage-TOM**“).

3.2. Änderungen der Anlage-TOM bleiben dem Anbieter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen und bedürfen der vorherigen Zustimmung durch den Auftraggeber in Textform.

§ 4 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

4.1. Der Anbieter unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber anvertrauten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Anbieter besteht.

4.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Anbieter unverzüglich hierüber zu unterrichten.

4.3. Der Anbieter trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß § 4.1 oder der Fehler gemäß § 4.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen § 4.1 oder § 4.2 sind unverzüglich in Textform nachzureichen.

§ 5 Übermittlung von Daten an einen Empfänger in einem Drittland oder in einer internationalen Organisation

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter Einhaltung der in Art. 44 ff. DSGVO festgelegten Bedingungen zulässig. Einzelheiten werden bei Bedarf in einer oder mehreren Anlagen geregelt.

§ 6 Unterbeauftragung weiterer Auftragsverarbeiter

6.1. Der Anbieter darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“) erbringen lassen.

6.2. Der Anbieter informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach

Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt. Im Fall eines begründeten Widerspruchs des Auftraggebers räumt dieser dem Anbieter eine angemessene Frist ein, um den vom Widerspruch betroffenen Unterauftragnehmer durch einen anderen Unterauftragnehmer zu ersetzen. Ist dem Anbieter dies nicht möglich oder dem Auftraggeber nicht zumutbar, ist die jeweilige Partei zur außerordentlichen Kündigung des Hauptvertrags aus wichtigem Grund berechtigt.

6.3. Der Anbieter wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Anbieter als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Anbieter ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

§ 7 Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Person Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Anbieter unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

§ 8 Kontroll- und Informationsrechte des Auftraggebers

8.1. Der Anbieter weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

8.2. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit kann der Anbieter auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Anbieter hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Weitere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) können zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus § 8.3 bleibt hiervon unberührt.

8.3. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Anbieter zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Anbieter darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen TOM abhängig machen.

8.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien die umzusetzenden Maßnahmen ab.

8.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

§ 9 Verarbeitung von Sozialdaten im Auftrag

Werden unter dem AVV Sozialdaten i.S.d. § 67 Abs. 2 SGB X (neu) im Auftrag verarbeitet, gilt dieser AVV mit folgenden vorrangigen Regelungen, wobei Daten neben personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DSGVO auch Sozialdaten i.S.d. § 67 Abs. 2 SGB X (neu) umfassen:

9.1. Bei der Übermittlung von Sozialdaten an einen Empfänger in einem Drittland oder in einer internationalen Organisation sind neben § 5 ergänzend § 77 SGB X (neu) und § 80 Abs. 2 SGB X (neu) zu beachten.

9.2. Die Anzeigepflicht nach § 80 Abs. 1 S. 1 SGB X (neu) vor Erteilung des Auftrags ist durch den Auftraggeber erfüllt worden. Handelt es sich beim Anbieter um eine öffentliche Stelle, hat dieser die Anzeigepflicht nach § 80 Abs. 1 S. 1 SGB X (neu) vor Erteilung des Auftrags erfüllt.

9.3. Handelt es sich beim Anbieter um eine nicht-öffentliche Stelle, stellt der Auftraggeber sicher, dass die besonderen Voraussetzungen für die Erteilung des Auftrags gemäß § 80 Abs. 3 SGB X (neu) gegeben sind, sofern sich die Verarbeitung im Auftrag nicht auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen bezieht, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann.

9.4. Liegen zu erwartende oder bereits eingetretene Störungen im Betriebsablauf bei Verarbeitungen im Auftrag vor, die sich auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen beziehen, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann, wird der Auftraggeber diese unverzüglich gemäß § 80 Abs. 5 S. 2 SGB X (neu) der Rechts- oder Fachaufsichtsbehörde mitteilen.

§ 10 Haftung und Schadenersatz

10.1. Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

10.2. Auftraggeber und Anbieter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

10.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei, zur Aufsichtsbehörde oder gegenüber Dritten gefährden.

§ 11 Kosten

Die durch Maßnahmen des Auftraggebers beim Anbieter anfallenden Kosten sind vom Auftraggeber zu tragen, soweit diese nicht mit der Vergütung nach dem Hauptvertrag abgegolten sind. Dies gilt insbesondere für durch Kontrollen und Inspektionen des Auftraggebers nach § 8 dem Anbieter anfallende Kosten.

§ 12 Laufzeit

12.1. Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer Anlage wird in der jeweiligen Anlage geregelt; ohne eine solche Regelung läuft die Anlage auf unbestimmte Zeit.

12.2. Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle Anlagen beendet wurden.

12.3. Eine Anlage endet mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser Anlage bedarf. Der Anbieter hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der Anlage verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform zu bestätigen. Sofern der Anbieter eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

§ 13 Fortgeltung und Überleitung von Altverträgen

Der AVV ersetzt mit Wirkung ab seiner Unterzeichnung die bestehenden Verträge nach § 11 BDSG. Haben die Parteien vor Abschluss dieses AVV Festlegungen nach § 1 vereinbart, so

gelten diese sinngemäß unter dem AVV fort, es sei denn sie werden durch Anlagen ersetzt, denen derselbe Verarbeitungsgegenstand zu Grunde liegt.

§ 14 Schlussbestimmungen

14.1. Sollten die Daten des Auftraggebers beim Anbieter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Anbieter den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Anbieter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

14.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

14.3. Sollte nur eine Bestimmung dieses AVV ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen unberührt. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch verpflichtet, unverzüglich Verhandlungen aufzunehmen mit dem Ziel einer Vereinbarung an Stelle der rechtsunwirksamen oder nichtigen Bestimmung, die deren Sinn und Zweck in rechtlicher und wirtschaftlicher Hinsicht am Nächsten kommt, insbesondere dem Charakter der Vereinbarung als Dauerschuldverhältnis zur Regelung datenschutzrechtlicher Belange gerecht wird.

14.4. Es gilt deutsches Recht unter Ausschluss des Kollisionsrechts; Art. 3 Abs. 3, Abs. 4 ROM-I-VO bleiben unberührt.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift
_____	_____
Name, Funktion Unterzeichner/in (in Druckbuchstaben)	Name, Funktion Unterzeichner/in (in Druckbuchstaben)

Anlage 1: Technische und organisatorische Maßnahmen des Unterauftragnehmers Ghostthinker GmbH (TOM)

Der Unterauftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Die beschriebenen Maßnahmen gelten für alle Orte, an denen die personenbezogenen Daten verarbeitet werden gleichermaßen. Sofern an einzelnen Standorten (z.B. eines Unterauftragnehmers) gesonderte Maßnahmen ergriffen werden, ist dies gekennzeichnet.

1. Vertraulichkeit

Zutrittskontrolle

- Die Server unserer Unterauftragnehmer stehen jeweils in einem Rechenzentrum. Die Sicherheitsvorkehrungen können den Agreements der Firma Hetzner entnommen werden.

Weitere Maßnahmen von Unterauftragnehmer Hetzner in den Datacenter-Parks in Nürnberg und Falkenstein:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- dokumentierte Schlüsselvergabe an Mitarbeiter/innen und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

Zugangskontrolle

- Mitarbeiter/innen des Unterauftragnehmers sind auf Basis der Vertrauensarbeitszeit beschäftigt. Das bedeutet, dass sie jederzeit Mobile Office in Anspruch nehmen können. Personen- und geschäftsbezogene Daten werden nicht lokal, sondern in cloud-basierten Speicherorten abgelegt. Darüber hinaus sind alle mobilen Geräte, die den Mitarbeiter/innen von Ghostthinker zu Arbeitszwecken zur Verfügung gestellt werden, durch eine Verschlüsselung gesichert.
- Die Mitarbeiter/innen der Ghostthinker GmbH verfügen alle über ein Programm zur automatischen Generierung, Verschlüsselung und Speichern von Passwörtern. Diese verfügen über eine festgesetzte Mindestlänge und Zeichenvariation.
- Abhängig von ihrer Funktion im Unternehmen erhalten die Mitarbeiter/innen einen Zugang zu den jeweiligen, zur Verrichtung Ihrer Tätigkeit notwendigen Programmen und Daten.
- Mobile Datenträger sind Unternehmenseigentum und verschlüsselt.
- Die Erteilung und der Entzug von Berechtigungen werden in einem internen Verzeichnis vom DST-Team erfasst und gepflegt. Alle 6 Monate wird das Verzeichnis auf Aktualität und weitere Erfordernisse überprüft.

Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Unterauftragnehmer sicher, dass unberechtigte Zugriffe auf das System verhindert werden.
- Der Unterauftragnehmer ist ein weitgehend papierloses Unternehmen. Alle Mitarbeiter/innen sind dazu angehalten ausschließlich digital zu arbeiten.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt zerstört (geschreddert).
- Für das Ausscheiden bzw. die Positionsänderung einer Person gibt es einen festgelegten Offboarding-Prozess, bei dem alle Berechtigungen und Zugänge entzogen werden.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Unterauftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Unterauftragnehmers

Datenträgerkontrolle

- Der Arbeitnehmer nutzt zum Transport oder zur Ablage von Videodaten externe Datenträger (mobile Festplatten, USB Sticks). Diese sind nach Vorschrift verschlüsselt.

Maßnahmen von Unterauftragnehmer Hetzner im Datacenter-Parks in Nürnberg und Falkenstein:

- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

Trennungskontrolle

- Produktiv-, Test- und Entwicklungssysteme sind physisch oder logisch getrennt.
- Bei einer Replizierung des Produktivsystems auf das Entwicklungssystem zu Testzwecken werden personenbezogene Daten anonymisiert.
- Durch Mandantenfähigkeit wird sichergestellt, dass die Daten verschiedener Kunden logisch, teils auch physisch, voneinander getrennt sind.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

Pseudonymisierung & Verschlüsselung

- Alle Passwörter werden nach aktuellem Stand der Technik ausschließlich verschlüsselt gehalten.
- Bei der Deaktivierung der zentralen Speicherung der Lizenzdaten durch die jeweilige Organisation werden die personenbezogenen Daten spätestens bei nächtlichen Wartungsarbeiten genullt.

2. Integrität

Weitergabekontrolle

- Alle Mitarbeiter/innen sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

Eingabekontrolle

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

- Es gibt ein mehrstufiges Backup-Konzept mit täglicher Sicherung der Dateien und vierstündiger Sicherung der Datenbanken.

- Zentrales Monitoring aller relevanten Systeme.
- Datensicherungen werden auf verteilten Systemen / Servern aus der Infrastruktur des Auftragnehmers aufbewahrt.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten.
- Einsatz von Festplattenspiegelung.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Einsatz von Softwarefirewall und Portreglementierungen.
- Dauerhaft aktiver DDoS-Schutz.

Rasche Wiederherstellbarkeit

- Der Unterauftragnehmer verfügt über ein Notfallsystem mit korrespondierendem Notfallplan.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

- Die Unternehmensleitung hat das Thema Datenschutz und Informationssicherheit durch die Einführung eines Datenschutzhandbuches und korrespondierendem Datenschutz-Managementsystems zentral verankert. Im Zuge dessen werden alle Mitarbeiter/innen des Unterauftragnehmers entsprechend, kontinuierlich zum Thema Datenschutz geschult.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.

Incident-Response-Management

- Der Unterauftragnehmer hat ein Notfall und Ticketsystem, das jeder Zeit per Formular und E-Mail erreichbar ist.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Incident-Response-Management ist vorhanden.

Auftragskontrolle

- Der Unterauftragnehmer hat einen Datenschutzbeauftragen und einen Informationssicherheitsbeauftragen bestellt.

Weitere Maßnahmen von Unterauftragnehmer Hetzner:

- Unsere Mitarbeiter/innen werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
- Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

Anlage 2: Festlegungen zur Auftragsverarbeitung

zwischen

Name + Adresse MO

(nachfolgend „**Auftraggeber**“)

und

Name + Adresse MO / DOSB

(nachfolgend „**Anbieter**“)

Die Parteien treffen zum Vertrag über die Auftragsverarbeitung ergänzend folgende Festlegungen:

§ 1 Gegenstand der Verarbeitung (Zutreffendes bitte ankreuzen)

☐ Der Gegenstand des Auftrags ergibt sich aus dem schriftlichen Hauptvertrag [Bezeichnung] vom [Datum].

☐ Der Gegenstand des Auftrags ergibt sich aus [sonstigen schriftlichen Dokumenten] vom [Datum].

☒ Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Anbieter:

- Bereitstellung eines Online-Portals zur Ausstellung von DOSB-Lizenzen
- Bereitstellung einer Datenbank zur Verwaltung der Daten von DOSB-Lizenzinhabern
- Erstellung und Visualisierung von Lizenzstatistiken

§ 2 Dauer des Auftrags (Zutreffendes bitte ankreuzen)

☐ Die Dauer des Auftrags ergibt sich aus dem schriftlichen Hauptvertrag [Bezeichnung] vom [Datum].

☐ Der Auftrag beginnt am [Datum] und endet am [Datum].

☒ Der Auftrag beginnt mit Unterzeichnung dieser Anlage und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von 3 Monaten zum Quartalsende kündbar. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt hiervon unberührt.

☐ Der Auftrag wird zur einmaligen Ausführung in folgendem Zeitraum geschlossen: [Angabe eines konkreten Zeitraums].

§ 3 Zweck der Verarbeitung (Zutreffendes bitte ankreuzen)

Die Tätigkeit des Auftragnehmers dient folgenden vereinbarten Zwecken:

- Bereitstellung eines Portals für eine einfache und zeitgemäße Beantragung und Verwaltung von DOSB-Lizenzen für Trainer/innen, Übungsleiter/innen, Vereinsmanager/-innen und Jugendleiter/innen und Ausbilder/innen online über das Wissensnetz
- Integration von personalisierten Daten über besuchte Aus- und Fortbildungen werden nach aktuellem Sicherheitsstandard ausschließlich mit einer verschlüsselten Verbindung (mind. TLS 1.2) übermittelt.
- Anbindung bzw. Integration der Lizenzstatistik 2.0, dem System für die Erstellung und Visualisierung von Lizenzstatistiken des DOSB, an das Lizenzmanagementsystem. Dem Anbieter werden zu diesem Zweck ausschließlich folgende Daten zur Erstellung der Lizenzstatistik übermittelt:
    - Lizenznummer

- Erweiterter Ausbildungsgang der Lizenzierung
- Geschlecht des Lizenzinhabers
- Die ersten beiden Ziffern der Postleitzahl des Wohnortes des Lizenzinhabers
- Geburtsdatum des Lizenzinhabers
- Ausstellende Organisation der Lizenz
- Datum der Erstausstellung der Lizenz
- Gültigkeitszeitraum der Lizenz.

§ 4 Kategorien personenbezogener Daten (Zutreffendes bitte ankreuzen)

Folgende Kategorien personenbezogener Daten sind Gegenstand des Auftrags:

- Personenstammdaten (z.B. Titel, Name, Vorname, Geburtsdatum, Geschlecht, Straße, PLZ, Ort)
- Verbands-/Vereinszugehörigkeit
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie (z.B. Lizenzverlängerungen, Fortbildungsmaßnahmen)
- Tracking Daten/Planungs- und Steuerungsdaten
- Statistische Daten (z.B. Ausbildungsgang, Gültigkeit)

§ 5 Kategorien betroffener Personen (Zutreffendes bitte ankreuzen)

Folgende Kategorien betroffener Personen sind Gegenstand des Auftrags:

- Trainer/innen mit DOSB-Lizenz
- Übungsleiter/innen mit DOSB-Lizenz
- Jugendleiter/innen mit DOSB-Lizenz
- Vereinsmanager/innen mit DOSB-Lizenz
- Ausbilder/innen mit DOSB-Lizenz

§ 6 Besondere technische und organisatorische Maßnahmen

Die Parteien haben für diesen Auftrag folgende, über die im AVV vereinbarten TOM hinausgehenden besonderen technischen und organisatorischen Maßnahmen festgelegt, deren Umsetzung vom Anbieter gewährleistet wird:

Die Zugriffsrechte im Online-Portal werden wie folgt geregelt:

- Der Zugang zum Online-Portal ist passwortgeschützt. Die Mindestpasswortlänge beträgt 12 Zeichen mit Passwortkomplexität (Buchstaben, Sonderzeichen, Ziffern).
- Die vom Auftraggeber auf dem Portal eingetragenen personenbezogenen Daten seiner Lizenzinhaber sind durch den individuellen und passwortgesicherten Zugang zum Online-Portal geschützt und abgesehen von den Administratoren des Dienstleisters, für niemanden außerhalb der Organisation des Auftraggebers einzusehen.
- Der Auftraggeber hat im Portal die Möglichkeit festzulegen, ob die personenbezogenen Daten nach der Lizenzerstellung gespeichert oder am Ende des jeweiligen Tages wieder verworfen werden sollen.
- Der Auftraggeber hat im Portal die Möglichkeit die Sichtbarkeit der gespeicherten personenbezogenen Daten seiner Lizenzinhaber für seine Unterorganisationen eigenständig zu regulieren.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift
_____	_____
Name, Funktion Unterzeichner/in (in Druckbuchstaben)	Name, Funktion Unterzeichner/in (in Druckbuchstaben)